Policy Analysis
No. 716 January 7, 2013

A Rational Response to the Privacy "Crisis"

by Larry Downes

Executive Summary

What passes today as a "debate" over privacy lacks agreed-upon terms of reference, rational arguments, or concrete goals. Though the stars are aligning for a market in privacy products and services, those who believe that rapidly evolving information technologies are eroding privacy regularly pitch their arguments in the direction of lawmakers, pushing for unspecified new rules that would cast a pall over innovation. These calls for ill-considered new laws threaten the remarkable economic conditions that have fueled the Internet revolution up until now.

Americans are torn between two historical and cultural traditions about privacy. The Puritan vision of true information transparency on the one hand lives uncomfortably with the frontier's promise of anonymity and personal reinvention on the other. When the Puritan vision encroaches too quickly on the frontier vision, it produces an emotional response—the "creepy factor"—that tends to recoil from innovative new uses of information. But "creepiness" often abates as familiarity grows.

We cannot solve the privacy "crisis" by treating information as the personal property of those to whom it refers or by adapting the systems for protecting copyright, patent, and other so-called "intellectual property" to personal information. But a related body of law explains and rationalizes what is going on with personal information and privacy: the more flexible solution of information licensing.

The licensing model recognizes that most information with economic value is the collaborative creation of multiple sources, including individuals and service providers. Rather than establish enforceable title to property, it assumes joint ownership and licenses specific uses based on mutual exchange of value.

Licensing is already implicit in most information exchanges on the Internet today. With minor enhancement, it could resolve many of today's perceived crises without resorting to inflexible and overreaching legislation.

Larry Downes is an Internet industry analyst. He is the author of the Business Week *and* New York Times *business bestseller,* Unleashing the Killer App: Digital Strategies for Market Dominance *and, most recently, of* The Laws of Disruption: Harnessing the New Forces that Govern Business and Life in the Digital Age.

CATO INSTITUTE

Between Congress, the European Union, and U.S. state legislatures, there are at least a dozen major proposed new laws in the hopper.

Privacy in 2012: State of Disunion

In 2011, I moderated a panel titled "Privacy, Personal Data and Publicness: Where Are We Heading?" at the Privacy Identity Innovation conference (PII).[1] As far as I could tell, we were heading exactly where we are every time we ask that question, which is over a cliff. Between Congress, the European Union, and U.S. state legislatures, there are at least a dozen major proposed new laws in the hopper, many of them aimed at resolving very specific presumed crises that threaten consumer privacy, including "supercookies," geo-location data, targeted advertising, and disclosure of data breaches.

If enacted and enforced, each of these proposals would have severe unintended consequences on the continued evolution of digital products and services. And none of them actually define what behaviors they are trying to regulate, or exactly why. What's the harm being remedied? And why do we think consumers won't continue to make clear what they do and do not want from service providers in the absence of new laws?

Much of this activity was spawned by an alarming report, "Protecting Consumer Privacy in an Era of Rapid Change," issued at the end of 2010 by the Federal Trade Commission (FTC). "[W]hile recent announcements of privacy innovations by a range of companies are encouraging," the Commission staff wrote, "many companies—both online and offline—do not adequately address consumer privacy interests."[2]

The report itself followed a series of free-form roundtables the FTC hosted the previous year, where self-appointed consumer advocates competed to outdo each other in raising the anxiety level over a privacy crisis that they said was imminent.[3]

But the report does little to define which "privacy interests" consumers are concerned about, and therefore what constitutes "adequate" protection of them. Many of the examples that regulators and others most often cite have to do with criminal activity—hacking, malware, identify theft, stalking—those are already illegal and outside the jurisdiction of the FTC. Other concerns have to do with the government's own collection, processing, and securing of citizen information—also outside the FTC's domain.

The 2010 report was preliminary. The FTC followed up in March 2012 with its final report, which reiterated the scary examples, emphasized the vague "principles" it called on companies to embrace, and ended with an overbroad appeal for legislation:

> The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation.[4]

Outside the FTC, there's a growing sense in Washington and Brussels that lawmakers need to do something—anything—to allay the privacy panics that pop up with innovative new social networking tools and mobile phone features. "[N]ow we have relationships with large corporations that are obtaining and storing increasingly large amounts of our information," Sen. Al Franken (D-MN) said in one his many recent hearings on privacy. "And we've seen the growth of this whole other sphere of private entities whose entire purpose is to collect and aggregate information about each of us."[5]

"We" don't know specifically what information we're concerned about, in what sense it is "ours," or why collecting and aggregating that information is wrong. But we need, nonetheless, "to legislate and make sure that our privacy protections are keeping up with our technology."[6] The attitude is to shoot first and ask questions later, even as the target continues to move faster than the gun sight.

The blustering of Franken and others highlights what makes most privacy discussions useless from the outset: the term "privacy" itself. The word conjures a great deal of

emotional baggage, as politically charged in its own way as net neutrality, gay marriage, or even abortion. Is it personal information? Intimate information? Identifying information? Or is the question subjective—information that an individual considers private at any given time, defined more by who wants to use the information than anything else? Rarely are two people talking about the same thing when they talk about privacy—not that that slows down the conversation.

One sign of hope that the privacy debate can move in a more focused and rational direction is the changing audience at privacy conferences. Increasingly, there are far more representatives of start-up companies focused on privacy-related services and many more participants from large technology companies, in particular from Europe and Asia.

When the debate was trapped in the bubble occupied by academics, journalists, regulators, and activists, it was just so much performance art. With actual money at stake, however, there are at least experiments that can illuminate what the real problems are, if not the solutions. PII 2011, for example, featured a dozen companies chosen for an "innovator's spotlight," which presented their plans to the audience in several showcases. Ten more start-ups presented at PII 2012.

That shift parallels recent reports that venture capitalists are investing heavily in privacy-related start-ups. In 2010, for example, Reputation Defender raised $15 million; TrustE another $12 million; and SafetyWeb, which lets parents monitor their children's online activities, raised $8 million. Those numbers pale in comparison to the amount being invested in the closely related category of security, but it's still a start.

Despite the difficulty of defining privacy or the nature of the crisis, the technological stars are aligning for a market in privacy products and services to emerge at last. As Moore's Law has worked its magic over the years, the data types and quantities of information that are cost-effective to process have grown exponentially. Static data has been supplemented with transaction data, and devices capable of processing it are proliferating at a fast pace. At this point it's cheaper to save data than it is to delete it, and most users do just that.[7] (The growth of sensors and other low-level devices that can collect real-time information may change that equation in the near future.) Much of the information that is aging—quickly—in aptly named data warehouses never gets queried for any purpose, nefarious or otherwise.

Today service providers are collecting data about each and every transaction in which they participate. It's worth repeating that the consolidation, personalization, and repackaging of that information is not something new or sinister—indeed, it has obvious benefits. It's a significant convenience not to have to reenter static information every time one returns to a website to browse, shop, pay bills, or search.

The more data collected, the more it can be used to improve everyone's transactions. Everything from eBay's seller ratings and other crowd sourced evaluation systems to Amazon's and Apple's recommendations based on similar purchases of similar buyers wouldn't be possible without the collection and processing of consolidated transaction data.

But with the personal computing revolution, the Internet, social networking, and the cloud, transaction data is now being dwarfed by the collection and processing of transient, and often intimate, information; a kind of Joycean stream-of-consciousness of the whole world. Much of it is entered into the datastream by users themselves. As of mid 2011, Twitter was processing 200 million tweets per day. It measures increases in the 1000s of percents.[8] Facebook averaged 3.2 billion "Likes" and comments generated by its 900 million users every day during the first quarter of 2012.[9] And who can count the number of blogs (let alone blog comments), emails, and other information-detritus?

Without much encouragement, and certainly no obligation, we are using social networks to digitize vast quantities of personal (though largely irrelevant and economically useless) information. Most of it can hardly be thought of as private, nor is there any risk that its inadver-

Today service providers are collecting data about each and every transaction in which they participate.

tent disclosure or use could harm or offend anyone but the truly paranoid. You post a link on my Facebook page to an article from a website that you read and found interesting. I check in at the office on FourSquare. A follower retweets your submission to the "things I learned from horror movies" trending topic. Who cares?

Well, some people care, although they have a hard time explaining why. There's a vocal minority who feel that any information collection, retention, or processing is an affront to personal autonomy and should be heavily regulated if not banned.[10] Activists want Web users to be allowed to sign up for "do not track" lists.[11] They want companies to disclose to all users every possible use of every possible data element before they collect it, and only collect it after a consumer has "opted in." In the foreseeable future, we may see proposals that every app on your mobile device stop before each data collection or processing activity to reassure itself of your continued consent.

What these rhetorically attractive ideas ("notice"; "transparency"; "choice") conveniently leave out of the equation is their immediate and catastrophic effect on the key innovation that made the commercial Internet so popular and so successful in the first place: advertising-supported services. Most websites are free to users. Google offers a nearly complete portfolio of application software and charges its users for almost none of it. So do Facebook, Twitter, LinkedIn, Groupon, and the rest of the old and new generations of Internet businesses. Search our databases! Store your email, photos, and videos on our servers! Make video calls with our software!

What motivates these businesses to drive as much traffic to their servers as possible? In the network economics of information, the more you exploit them, the more valuable their companies become. But not because users pay them directly. Rather, it is because their use makes the services more valuable to others.

For the most part, of course, those others are advertisers. The revolution in free services and software that has unleashed much of the computing genius of the last decade has been built largely on the back of advertising.[12] In 2011, for example, Google earned 96 percent of its revenue, or roughly $28 billion, from advertising.[13] And there was nothing new about that success—the earlier media revolutions of radio and television were financed exactly the same way.[14]

With most Internet services, the user is the customer, but the revenue comes from those who have an interest in accessing the right users. And the more accurate and detailed the information that service providers collect, from the largest possible user base, the more valuable the information becomes. So the incentives are there for service providers to make their products more compelling all the time, both to attract larger groups of users and to provide opportunities for those users to engage ever more deeply with the products, generating ever more data with which to impress advertisers.

Analyzing how many users a service has, how much time they spend with it, and what interesting things they do while they are there are skills at the core of successful Internet companies. Understanding user behavior, after all, translates to more ad spends and higher ad rates, generating both competitive advantage and revenue.

The importance of robust and detailed user information cannot be overemphasized. Unlike e-commerce sites selling products, social networking applications don't exist at all without user information—Facebook, Twitter, Yelp, even Craigslist and eBay are literally nothing without user-supplied content. Attracting users, giving them more things to do, and keeping them happy are not just customer service imperatives. They're a matter of life or death.

It's important to dispel right from the start some persistent myths about how advertising actually works. The marketing of transaction data is far more complex than advocates for more government regulation of privacy would have us believe. It's not "your" information that's being sold. First, the information is collected and stored by the service with your permission. If the data ever was "yours," you freely traded your interests in it. For most of the Internet's billion users, the exchange is a good one, generating

There's a vocal minority who feel that any information collection, retention, or processing is an affront to personal autonomy and should be heavily regulated if not banned.

far more value for users than the costs of supplying and parting with the information.

Data being processed for advertising isn't "yours" in a second sense: It doesn't identify you as the source. Search engines such as Google don't sell information about what individuals searched for, and advertisers don't then turn around and advertise to those individuals based on what they have learned about them. Google doesn't even know "who" is doing the searching, only that the searches originated from the same computer. Google keeps track of the activities of that computer (which could be used by one person, a family, the patrons of a library, or a bot), and it does so only by storing cookies on the computer that maintains the connection.

But the cookie doesn't contain identifiable information about the user—the name, address, and so on. And once you delete a cookie, the data collection has to start all over again. (Your searches will get less streamlined if you do, as Google's software will make worse guesses about what you're actually looking for.)[15]

More to the point, ads you see on Google search results or other applications only appear to be optimized as personal messages. In most cases, the services and their sponsors don't make use of the individual cookie data, or at least not on its own. Say you searched for "carpet cleaners in Berkeley, CA." Google doesn't sell that fact to carpet cleaners in Oakland, who then pass along an advertisement to the computer of whoever typed that search. The actual science of advertising is both more and less sophisticated than that.

For advertising to work, suppliers need the preferences, habits, and transactions of large numbers of users, which are consolidated, mined, and analyzed to find patterns and common behavior. (Gender and zip code are the most valuable pieces of identifying information—names and addresses are of little help.) Once all that information is compiled, it can be compared to the practices of a particular (but unidentified) user, who can then be served with ads more likely to be relevant to his interests. The better the science, the more the advertising appears to be personal. But it's still only the illusion of personal.

Focus is valuable to consumers as well as advertisers. More focused ads mean sellers waste far less time advertising the wrong things to the wrong people.[16] Nineteenth century retailing pioneer John Wannamaker famously said that half his ads were wasted, he just didn't know which half.[17]

Not much has changed. I keep a recycle bin right next to the mailbox, where nearly all of my delivered mail goes without being opened. I'm not against ads; I'm against ads for things I don't want. And I often don't know what I want until I see an ad that helps me realize which is which. Steve Jobs famously said, "A lot of times, people don't know what they want until you show it to them."[18]

Put another way, advertisements are offers. Those that are perceived as "ads" are offers that are at least slightly off. But an ad for the right product or service, offered at the right time to the right person at the right price, isn't an ad at all. It's a deal.

Personal results—or rather, results that appear personal—require group input. That's where the real value of data collection is, not in separating out the information of any particular individual. On their own the Amazon purchases of one customer are of little use in helping the company suggest other products that are likely to be of interest. That data must be compared to the purchases of everyone else before the "targeted" response can be meaningful.

The more data collected, the more valuable the collection, and the less reliance placed on the individual's data. In that sense the more information we allow to be processed, the more privacy we actually get in the form of obscurity. That, of course, is just one of the many privacy paradoxes that confound regulators and worry businesses.

Historical Roots of Privacy Panics: Hester Prynne vs. Davy Crockett

Understanding how information is actually collected and used would go far toward

Search engines such as Google don't sell information about what individuals searched for.

For most consumers and policymakers, privacy is not a rational topic.

freeing the "privacy debate" from the rhetorical sinkhole in which it has been trapped. Yet having that conversation seems impossible. Why? The short answer is that for most consumers and policymakers, privacy is not a rational topic. It's a visceral subject, one on which logical arguments are largely wasted. Americans seem wired to react strongly and emotionally just at the mention of the word "privacy," or the suggestion that some new technology is challenging it.

What sets in seems more often than not a panic response, as we worry that the game is up and our last remaining shred of personal autonomy has just been undone by products and services we don't understand, in part because they didn't exist yesterday and are only in prototype today. As science fiction author Arthur C. Clarke wrote in 1961, "Any sufficiently advanced technology is indistinguishable from magic."[19] And we know how locals often respond to those who wield magic.

Consider one example of the life cycle of a privacy panic: the blow-up in 2011 over Apple's geolocation files on the iPhone. Researchers "discovered" a file on the iPhone that appeared to be keeping track of cell towers and WiFi hotspots (not, as many said, GPS data) used by the device. Journalists and lawmakers jumped to the conclusion that the file was tracking the locations where the user's phone had actually been, making it possible for Apple to "spy" on its customers. The "secret" nature of the file, plus the potential for embarrassment if its contents were revealed by Apple (perhaps to law enforcement, perhaps to a divorcing spouse, or perhaps just out of spite), raised an alarm.[20]

The story exploded into immense proportions within hours, with news outlets reporting user outrage[21] and members of Congress, fuming, calling for hearings[22]—and, at the hearings, for new legislation, enforcement actions by the FTC,[23] and other corrections to what was clearly a privacy apocalypse.[24] Apple said nothing for a few days—researching, it turns out, what the file actually was—leading to even more anger at their corporate arrogance.[25]

In the end the whole thing turned out to be nothing. The file wasn't storing information about where the user had been, or even where the phone had been (Apple doesn't know who is holding the phone, obviously). The file was part of a crowdsourced database of connection points that other phones with similar usage patterns had made use of recently. It was being stored on the iPhone in the event that the user invoked a service that required knowledge of the phone's location (directions, area restaurants, etc.).[26]

The file was just a backup in the event a ping to the GPS satellites didn't work or responded too slowly. As the company made clear, "Apple is not tracking the location of your iPhone. Apple has never done so and has no plans to ever do so."[27]

But logic and facts play little part in an emotional response. A week after Apple explained the file's true nature, I spoke on an NPR news program with Sen. Al Franken and the FTC's chief technologist, Ed Felten.[28] Both of them continued to describe the incident as one where Apple was tracking the location of its users and failing to disclose that fact. Whether they simply hadn't read Apple's explanation or didn't believe it, both acted as if the answer had never been given.

Franken, who had already scheduled a hearing, stuck to his script: "We had this thing with Apple with iPhones and iPads," he said on the program, "that were tracking your location and then storing it in an unencrypted way on a file, and let's say you hooked up to your own laptop and all that information then went on your laptop, so it had stored this information for, you know, almost a year of pretty much everywhere you'd been with your device. And we're talking about other kinds of mobile devices as well and privacy concerns."[29]

But Apple was not tracking "your" location, or even of the location of your device. It wasn't tracking anything at all. Both of them should have known better, and almost certainly did. But the story was too good, and the visceral reaction too powerful not to use in pursuit of unrelated interests. In Franken's case, it's the passage of some new privacy leg-

islation—he seems not to care especially which of several proposals moves forward. For the FTC, the greater the panic over privacy, the more likely the agency will get new authority and new funding to enforce new rules. Like any enterprise, they want to increase their market share.[30]

The vagueness of demands for new laws and regulations would be comical if it weren't so dangerous. Americans don't know what they want when it comes to privacy; or rather, that what they want depends on when and how the question is asked. We want to protect victims of domestic abuse from being stalked, for example, and so we insist that search engines, cell phone providers, and social networks delete identifying information immediately. But we also want the police to catch those who are doing the stalking, and so we also insist that information collectors retain identifying information.[31]

The result is a regulatory whipsaw. In 2008 the House Energy and Commerce Committee pressed Verizon, AT&T, Time Warner, Comcast, Microsoft, Yahoo, and Google to reduce the length of time they retained customer transaction data, which many of the companies voluntarily agreed to do.[32] Yet in 2011 the House Judiciary Committee advanced a bill (with 40 cosponsors) that would require these same companies to increase the length of time they retained the exact same data, and make it available without a warrant to law enforcement agencies investigating a variety of crimes.[33]

Even without actual lawmaking, simple threats have led to unhelpful responses. Under pressure from the House in 2008, for example, Yahoo changed its data retention policy from 13 months to 3 months.[34] But when Congress and the Department of Justice pressed for longer retention in 2011 in the name of effective law enforcement, the company changed its policy again, this time from 3 months to 18 months.[35] Context is everything, and the context is only clear after the fact. But laws and regulations by their nature deal with future situations. We're therefore doomed to be, generally speaking, unhappy. Or at least uneasy with any legal remedies.

There may be some solace in recognizing that there's nothing new about these privacy paradoxes. American culture has long maintained inconsistent attitudes toward privacy, simultaneously embracing secrecy and transparency with equal passion.

The source of that dichotomy has deeply historical roots. On the one hand, the whole point of frontier life (which many historians believe defines the American experience) was the ability to go west, shed personal baggage from your past, and redefine yourself however you wanted. The kind of "rugged individualism" practiced by Henry David Thoreau and extolled in the essays of his friend Ralph Waldo Emerson meant one was judged by his deeds, not the accidents of his birth or his past. Davy Crockett, whose modest achievements as a frontiersman, congressman, and soldier were elevated to mythic status as the self-made "King of the Wild Frontier," perhaps best epitomizes the spirit of the wide open American West.

Ranchers and farmers could be as anonymous as the height and opaqueness of their fences,[36] and as eccentric, too. If the neighbors got too nosey, one just moved farther west. Joseph Smith, founder of the Mormon religion, believed himself to be a prophet, a view that was met with hostility in his native New York. Smith moved west to Ohio, Missouri, and then Illinois, where he was assassinated.[37] So his followers headed for the wilderness and settled in Utah where they could do as they felt compelled without interference, at least until the line of settled frontier caught up with them decades later.

Back East, the original colonies were largely settled by Puritans, who practiced a particularly extreme form of what today is referred to as transparency. God saw everything, so why not the rest of the community? Perhaps the most evocative picture of the lack of privacy in early American life is the one painted in Nathaniel Hawthorne's *The Scarlet Letter*, where Hester Prynne's punishment for extramarital sex (evidenced by the birth of her child) is to be forced to wear a giant letter A (for adulterer) on her chest.[38]

American culture has long maintained inconsistent attitudes toward privacy.

The digital revolution has all but erased the cost barrier to collecting and processing social information.

That the father of her child is the town's fire-branding preacher, who speaks most passionately against Hester, is Hawthorne's way of suggesting the hypocrisy of the transparent Puritan village. But hypocrites or no, these were some seriously mandatory social networks.

Frontier and Puritan America coexisted in a kind of uneasy peace, with the law of the East occasionally visited on the lawless West, which was mostly left alone if for no other reason than the cost of enforcement. The federal government unsuccessfully attempted to suppress the "Utah Rebellion" in the 1850s, for example, but it was not until completion of the transcontinental railroad though Salt Lake City in 1869 that pressure began to build on the Mormons to abandon polygamy and accept a secular government. The Church banned polygamy in 1890, and Utah became a state six years later.[39]

With the closing of the American frontier (Frederick Jackson Turner pegged the date at 1890[40]), one would have thought the Puritans would reassert Calvinist transparency on the whole country. But the industrial revolution brought forth other ideas. The anonymity of the frontier was replaced by the anonymity of city life.[41] In the metropolis, there were just too many people to keep track of or to assert moral authority over.

Hester Prynne would have been free to walk the streets of 19th and 20th century Manhattan anonymously. No one would know or care how she lived her life, which would perhaps be fatal. Where *The Scarlet Letter* captures the claustrophobia and hypocrisy of Puritan village, the archetypal story of dangerous anonymity and isolation in industrial life is that of Kitty Genovese, a New York City resident who was brutally raped and murdered in an alley in 1964 while neighbors all around did nothing, not even calling the police. The story has been exaggerated and mythologized, but even its persistence as myth underscores modern fears that industrial life dehumanizes urban residents.[42] That is, it gives them too much privacy, to the point of anomie.

Before social networks and smartphones, cities were impersonal, amoral, and paranoid. Early in Joseph Heller's 1974 novel, *Something Happened*, the narrator captures the spirit (or dispirit) of the company man: "In the office in which I work, there are five people of whom I am afraid. Each of these five people is afraid of four people (excluding overlaps), for a total of twenty. . . . "[43] And so on until it becomes clear that everyone in New York is afraid of everyone else.

In economic terms, we could say that early urban life raised the cost of collecting, storing, processing, and accessing the kind of information we need to decide whether or not to network with each other. Absent computers and digital technology, the price was too high. The default—that is, the lowest-cost response—was to do nothing, whether to call the police or to trust one's coworkers, let alone strangers. "Mind your own business" is an equation as much as it is a cliché.

Meanwhile, the Puritan ideal lived on in the suburbs, where, according to an equally persistent mythology, people kept their doors unlocked and everyone knew everyone else's affairs. Whether that was a utopian myth (*Leave it to Beaver*) or a dystopian one (*Peyton Place*) depended on, well, depended on nothing, really. Americans have always been comfortable supporting contradictory views of privacy and its pluses and minuses.

In both town and country, however, the digital revolution has all but erased the cost barrier to collecting and processing social information. Now that we can have it all, we're unavoidably faced with a true privacy paradox. On the Internet, we live in both city and suburb, Puritan village and frontier wilderness, at the same time. We want—demand—our privacy, but we also expect to be able to share whatever information we want, from the sublime to the ridiculous, with whomever we want, and to do so free of charge. Often, the tension between these two powerful desires leads to contradictory behavior and conflicting legal standards.

The Puritan part of our minds (the part that invented capitalism, according to Max Weber[44]) wants to know everything about everyone else, the better to decide whether

and how to interact with them. Transparency is a virtue, and not just for corporations and governments. The more information we can collect and process about everything and everyone, the easier it is to decide with whom to interact and how to behave. Information, on this view, is the lubricant that keeps the machinery of society humming.

The frontier part of our minds, on the other hand, wants the option to be anonymous on demand, "to be let alone" in the famous formulation of Samuel Warren and Louis Brandeis—or the "right to be forgotten" as it's now being called in Europe.[45] The frontier mind recognizes, although often vaguely and viscerally, that there is something profoundly American about keeping to oneself, and it resents the intrusion into our personal lives of anyone we don't explicitly invite (an invitation that can be revoked either on whim or further reflection).

The pioneer view of personal autonomy was a central motivator for many of the groups who migrated to the United States, including, oddly enough, the Puritans, who had suffered enough interference with their beliefs and practices by the Crown to pack up and sail to the New World.

That peculiar version of a right to privacy—asserted against the government but not each other—is baked into the U.S. Constitution. Many of the most potent safeguards provided by the Bill of Rights in particular limit the ability of governments to demand information from the people. In response to the heavy-handed practices of America's colonial overseers in England, for example, the Fourth Amendment prohibits unreasonable search and seizure of "persons, houses, papers, and effects."[46] The First Amendment bans Congress from legislating on matters of religion or speech,[47] two aspects of individual identity that are particularly "private." The post–Civil War amendments expanded the Bill of Rights, extending its protections to former slaves and including state and local governments in bans that had originally applied only to the federal government.

But, again, these privacy protections explicitly bar intrusions by the government. The Constitution says nothing that even suggests a limit on how much information can be collected by businesses or other citizens, no matter how intrusive or how it is used. Except for a few specifically legislated exceptions, Americans have no general right to privacy against anyone other than the sovereign.

So Americans have always experienced privacy as a kind of Manichaean duality. Perhaps that explains why every survey taken on attitudes to privacy in the digital age suggests Americans are deeply concerned about their personal information online even as they casually give up whatever data is asked of them, often with no idea who is doing the asking or the purpose of the collection.[48]

The external conflict between Puritan and frontiersman, between Hester Prynne and Davy Crockett, has now been internalized. We're capable of living with our discomfort, which is saying something. We demand the right to have our every trivial thought broadcast to the Twittersphere, and to have attention paid to it. And then we recoil in panic at novel technological developments (geolocation tracking, super cookies, and facial recognition) that expose some new aspect of ourselves to the world.

The internal conflict often masks innate hypocrisy. Many people want privacy from outsiders but reserve the right to demand full disclosure from those with whom they interact on a daily basis. But what's good for the goose is good for the gander. Those who most adamantly insist on legal tools to erase their past would likely be outraged were they the victims of someone else's false or misleading presentation of self.

You may not want future creditors to know about your poor payment history, or for potential employers to find out about your criminal record, or for someone you hope to date hearing about your previous marriages. But these are essential facts if others are going to, respectively, loan you more money, hire you to a position of responsibility, or move in with you. The desire for privacy is often a desire to protect ourselves from the negative

Many people want privacy from outsiders but reserve the right to demand full disclosure from those with whom they interact.

consequences of our own behavior.

In that sense, privacy isn't a human right—it's a limit on the rights of those who have to deal with us. Privacy comes at a price. The more of it we have, the more risk to which we expose everyone else. In commercial transactions, banks and insurers offer protection against that risk (often at a steep cost). In social interactions, all we have to fall back on are limited safeguards of tort law, which assigns liability to dangerous behavior only if it causes calculable harm, and criminal law, which punishes the most egregious acts, including assault, theft, and large-scale fraud.

There have been periodic efforts in U.S. history to expand the constitutional right to privacy from government intrusion into a broader protection that can be asserted and enforced against technological innovations employed by businesses, the press, and other individuals. For the most part, however, these efforts have failed to overcome the Puritan's economic and cultural biases for transparency. Warren and Brandeis, for example, began their crusade in response to the novel challenge raised by newspaper photos exposing the social and personal lives of the well-to-do. But they never argued that their revolutionary "right to be let alone" actually existed in American jurisprudence. Instead, they hoped that outrage with an overly familiar press would rally general support for new laws to create it.[49]

Following publication of "The Right to Privacy," some state courts did tinker with new legal claims for "false light," "invasion of privacy," and other privacy-related torts. But efforts to create a general right to privacy largely sputtered out. And as the U.S. Supreme Court moved to shore up First Amendment protections for a press under siege during the Civil Rights movement, whatever was left of these novel rights was further marginalized.[50]

Today, the U.S. press and other nongovernmental actors enjoy wide freedom to report true facts, even those obtained through invasive technologies that would have seemed inconceivable to Warren and Brandeis. The Constitution has spoken: the need to know even personal details of the lives of our celebrities, including political and cultural figures large and small, outweighs Warren and Brandeis's desire for new laws to ensure "propriety" and "decency."[51]

Privacy isn't a human right—it's a limit on the rights of those who have to deal with us.

Measuring the Creepy Factor

Today's privacy crisis is a function of innovation that happens too quickly. Given the accelerating pace of new information technology introductions, new uses of information often appear suddenly, perhaps overnight. Still, after the initial panic, we almost always embrace the service that once violated our visceral sense of privacy. The first reaction, what I call the "creepy factor," is the frontier response. It doesn't last long. The Puritans reassert their rational order more quickly all the time.

As noted earlier, large-scale data collection, like the urbanization of America, in some ways contributes to privacy even as it challenges it. The more information available about more people, in other words, the more privacy we get as anonymous members of various groupings. Perhaps the biggest reason for today's resurgent and generalized privacy anxiety is that it just doesn't seem that way. When a novel information service *appears* to have zeroed in on one's deepest darkest secret preferences, it's hard to resist a strong emotional response. But there is almost always an explanation that, when understood in context, takes the creepiness out of the equation.

How, for example, did Google know when I searched for "War Horse" that I was looking to buy tickets to a performance of the play in San Francisco? (Answer: my IP address identifies the service provider for my computer as Comcast in Richmond, California.) How does CNN know who my friends are, and what stories on the CNN website my friends have recently read? (Answer: my friends tagged the stories on Facebook, which actually controls that part of the screen.)

Better targeting of ads and other content,

unfortunately, often evokes a visceral response, one that is by definition not rational. When we imagine the specter of a kind of corporate Big Brother, the frontier mind kicks in, ready to saddle up and head west to avoid the prying eye of Puritanical software. Or worse, it can lead us to fretful and panicked calls for immediate legislative solutions that would reign in what are in fact entirely innocent and impersonal technologies that only simulate invasive human behavior, and that do so to our economic and social benefit.

Gmail users, for example, see ads along the top and side of the screen advertising products and services that often relate to the contents of recent emails and conversations. It's all software. We know intellectually that there's no vast army decamped at some Google Ministry of Love reading through the messages looking for opportunities to connect them to contextual advertising. But the software has gotten so good at interpolating our messages that it begins to look personal.

That's the moment when the creepy factor comes into play. Something happens that you didn't expect, or hadn't experienced before, and you think, "How did they know that?" Right now, my Facebook page is showing me photos of three people "you may know." I know all three. For two, the connection is obvious. For the third, the connection is eerily indirect. Until I understood what mundane data elements connected all three to me, I felt uneasy about Facebook. The company seemed to be an actual person, and a sinister one at that.

As we record more information in digital form in hopes of sharing it with our intimate contacts and less enthusiastically with advertisers who pay for the services we love, it's inevitable that more of these visceral responses will occur. When specific data is used in novel ways, the initial response is often to be creeped out.

So let's try to take the emotion out of the equation, or, at least, account for it in hopes of a more rational conversation about what, if anything, needs to be done to manage the creepy response. We can begin by restating the problem simply: the more personal the information used by an advertiser or service provider, the more emotional our response to its use:

$$P \rightarrow E$$

where P = personal and E = the degree of emotional response.

The creepy factor, however, is the response to a novel use of information to provide a seemingly personalized response. Over time, the creepy factor decreases. Most users are now accustomed to customized Google search results, specific Gmail ads, and prescient Facebook recommendations. They no longer creep us out. The diminishing emotional response can be represented by dividing the degree of emotional response by a second variable, F (familiarity), so:

$$P \rightarrow \frac{E}{F}$$

If consumer response to a particular information practice does not become less emotional over time, this suggests that the negative response is not a function of novelty but of genuine discomfort. Put another way, an information use that does not seem less creepy over time may be one that consumers believe imposes more cost to privacy than it provides in benefits elsewhere. That still doesn't mean a regulatory intervention, specific or otherwise, is required. Regulations impose costs of their own. Often the more efficient solution is for consumers to vote with their feet, or these days with their Twitter protests. As social networking technology is coopted for use in such campaigns, consumers have proven increasingly able to leverage and enforce their preferences.

In Europe, the default rule is almost the reverse—governments don't wait for true market failures, but instead protect vaguely defined general privacy rights against corporations on behalf of the citizens. This is one reason, and an important one, that most data processing innovations of the last 25 years have taken place in the United States. Entrepreneurs who

The creepy factor is the response to a novel use of information.

want to launch a new application or service that collects, analyzes, and processes information need not apply to any government agency for permission.

Indeed, for companies in the United States, adopting any kind of privacy policy (except as their service may apply to children) is entirely voluntary. The FTC can only bring enforcement actions when a company promises to treat information one way but actually uses it in another, and only when such behavior rises to the standard of an "unfair or deceptive" misrepresentation that causes actual harm; that is, when it approaches the legal definition of fraud.[52]

When new applications stimulate our creepy response (and more of them will enter the market all the time thanks to the technology trends mentioned above), the critical policy question then becomes what we do during the initial, emotional response period, when creepiness is high.

Consumers either adjust to new information use or act through the market to change the practice.

In the absence of premature interventions by regulators, in nearly every case consumers either adjust to what is an essentially inert new information use or act through the market to change the practice. Consumer-enforced change is frequent—recent examples include the cancellation of Facebook Beacon and Google Buzz, and Apple's modifications to the geolocation files stored on consumer devices. When consumers objected strongly to how these services were using information, the companies either modified their practices or canceled the service altogether.

In 2011, to take a specific example, LinkedIn users revolted against a new feature called "social ads," in which ads for a particular product or service included the profile photos of contacts in a user's network who recommended it.[53] The creepy factor was apparently too high, and the company quickly agreed simply to list the number of network members who recommended the advertised product.

The recommendations of one's contacts could always be seen by reviewing their individual profiles, but combining that information with ads apparently crossed a line. "What we've learned now," said Ryan Rolansky, the company's director of product development, "is that, even though our members are happy to have their actions, such as recommendations, be viewable by their network as a public action, some of those same members may not be comfortable with the use of their names and photos associated with those actions used in ads served to their network."[54]

This may be an example where constructive engagement with a service provider led to quick resolution—true market success. On the other hand, it's possible that with a little more familiarity to LinkedIn users, the creepy factor would have dissipated, and on balance provided more benefit than cost. The more "social" the ads at LinkedIn, after all, the more the company can charge its advertisers, keeping subscription fees lower and encouraging a larger and richer network.

Choosing the more expensive solution was a trade-off LinkedIn users made, but it was still better than forcing through new laws banning the use of photos in ads or some similar remedy. In response to another privacy panic, California recently passed a law prohibiting employers from forcing employees or job applicants to provide access to their "social media" accounts. But as legal scholar Eric Goldman points out, the law, while well-intended, was poorly drafted, and is certain to cause negative, unintended consequences if not corrected. For one thing, "social media" was defined so broadly that it effectively covers all electronic content, whether personal or employment-related.[55]

For those who naturally leap first to legislative solutions, it would be better just to fume, debate, attend conferences, blog, and then calm down before it's too late. Future innovations hang in the balance.

Unfortunately, the mainstream media often fans the flames of the emotional response, raising the value of E. The press has strong financial incentives, after all, to amplify and echo the creepy factor once it appears. That, at least, has been the repeated experience of the last decade. Outrageous stories of corporate and government information malfeasance are surefire attention-getters. It's no surprise that privacy-

related stories are often cast in that light, even when the facts are nowhere near so clear-cut.

Consider the *Wall Street Journal*'s What They Know series,[56] written by veteran reporter Julia Angwin. Angwin's award-winning stories investigate the actual information collection and use practices of a wide range of corporate and government entities, ranging from the largely innocent to the simply criminal. What they Know is a rare example of investigative journalism in technology reporting, and the source of important findings and discoveries.

While the series has helped to stimulate more mature conversations about privacy, its rhetorical style is often counterproductive. Angwin regularly stacks the deck and oversells the lede, crossing the line from reporting to commentary. Consider a *What They Know* story from 2010, which carries the headline "The Web's New Gold Mine: Your Secrets."[57]

The headline alone signals both a point of view and a conclusion. Is information collected by websites "yours"? And is it really "secret" or did you reveal it, perhaps over time or in different component parts? The phrase "gold mine," likewise, conjures an enterprise that, when successful, will generate enormous profits relative to cost. We know before reading the story that whatever gold is being mined, the miners are not to be trusted.

But headlines are not the story. Let's look at the first sentence:

> Hidden inside Ashley Hayes-Beaty's computer, a tiny file helps gather personal details about her, all to be put up for sale for a tenth of a penny.

The article, in case you didn't guess from the lede, is about the use of cookies. Cookies are data files that Web browsers store so that sites can record information about navigation and use by the particular computer on which the cookie is stored. When a user of that computer returns to the site, his or her browser sends the site a copy of the cookie, which allows the site to customize itself—highlighting links that have previously been clicked, for example, or pre-populating sign-in or other data fields with prior entries.

A strong connotation of this sentence is that factual information about Ashley is traded at a low price, passing hand-to-hand among heaven-knows-who, on a shady personal information market. This is a common, mistaken assumption about how advertising works.[58] In fact, it is advertising networks that use the information to direct ads her way. The only way for the companies doing the advertising to discover personal information about her is for her to click on one of their ads and begin interacting with them.

Whatever the ethical implications of more advanced uses of cookies, they have been a technical feature of web browsers from the beginning. Their useful attributes cannot be seriously doubted. They have never been held to be illegal.[59]

So does my navigation of a site's pages really constitute my "secrets"? Are mouse clicks even "personal" details? (The data in a cookie is not linked to a specific, identifiable person, as the story later makes clear.) Are cookies "hidden" from users "inside" our computers? (They can be viewed and deleted through the browser's control options; they can also be refused generically or by type of requesting site.) In what sense are they "tiny," and why does that matter?

According to the article, cookies and "other surveillance technology" "know" things about "you." They collect "your information" ("yours" both in the sense of being about you and being property which belongs to you), which is then "sold" to advertisers. This seems neither surprising nor dangerous, but in the hands of a skilled advocate, even the most inert technology appears weaponized. A few paragraphs on, Angwin writes: "One of the fastest-growing businesses on the Internet, a *Wall Street Journal* investigation has found, is the business of spying on Internet users."

Well that is certainly one interpretation of the article's findings, and clearly the one Angwin and her editors want readers to draw. From the article's details, however, what actually seems to be new—what the *Journal*'s investigation "found"—is that service providers are

In the hands of a skilled advocate, even the most inert technology appears weaponized.

The Internet is just picking up where television once blazed a trail.

getting better at making economically beneficial use of the data that cookies and "other surveillance technology" have been collecting all the time. Beneficial to users as well as marketers, no less. Again, the ads pay for the free services.

Journalists are certainly free to beat their readers over the head. Most *Journal* readers, I suspect, prefer writers who lay out the facts and let them draw their own conclusions—or at least wait until the facts are established before editorializing in a news story. Given the general climate of creepy factor responses to Internet privacy, Angwin's language doesn't simply push the emotional button—it wires it to a car battery. To the extent that "What they Know" has discovered misleading, fraudulent, or otherwise illegal activities, Angwin rightly deserves the accolades her series has received. But why not give readers credit for being able to decide for themselves when data collection and use is good, bad, or somewhere in the middle?

Just as an exercise, let's rewrite that first sentence in neutral language, and see how the facts uncovered by the investigation lose some of their menacing implications:

> The Web browser on Ashley Hayes-Beaty's computer is set to accept cookies, files that site operators use to keep track of how users navigate their pages, both to save time on return visits and to offer more relevant advertising that helps pay for Web sites' operations.

Because most of the uses of personal information that trigger the creepy response are related to advertising, it's also worth noting that what's going on here isn't so much new as it is an improvement. Rather than simply pushing products, marketing long ago shifted to wrapping products inside solutions to larger consumer problems. Ads are now designed to appeal to more basic human aspirations or anxieties, and to suggest, often subtly, that the advertised product will fulfill or resolve those feelings.

The clearer a particular demographic group's feelings are understood, the better the ad can target their needs. That's all that's really involved in targeted or behavioral advertising—it uses contextual information to place a consumer in a group with common characteristics (age, sex, zip code) and then directs ads to them that are more likely to speak to that group.

The Internet is just picking up where television once blazed a trail. In the 1960s, television became the ubiquitous technology of what Marshall McLuhan called "the global village"—the prototype for social networks.[60] Those who are fans of "Mad Men" get the advertiser's view of the origins of targeted or behavioral advertising, albeit one filtered through a cloudy highball glass.

For marketers, the direct and visual properties of the medium made it possible to get inside the heads of viewers in ways print and radio simply couldn't approximate. Marketers, in short, learned to stop selling products and start selling solutions, often to deep-seated problems.

Consider some of the taglines from the early days of TV: "Does she or doesn't she?" (gray hair/aging). "We bring good things to life" (electric appliances/modernity) "Even your best friends won't tell you" (mouthwash/bad breathe). If those problems are actually existential and unsolvable, so much the better—consumers (the modern understanding of the term originates here) would have to keep buying forever, urged on by the promise of "new and improved."

The creepy factor was born in these ads. Watching television in the 1960s, it may have frightened viewers to see a commercial for instant coffee or laxatives or dandruff shampoo that emphasized the angst of the pre-purchasing characters—those who made bad coffee or had flakes on their clothes, just as they worried they also did. How did the television know what was making (some of us) anxious?

But over time, we adapted and moved on. We look at those old commercials now with nostalgia. How quaint and how impersonal they seem. But at the time they were nothing short of revolutionary, and even scandalous.

I have personal experience with the creepy factor, as most everyone does. In the early 1980s, I was a regular business traveler, taking four to six flights a week as part of my job as a systems engineer for a large consulting firm. I was a charter member of many airline frequent flyer programs which, like the Google+ and Spotify of their day, were initially by invitation only.

It was a foregone conclusion that that information would be put to some use other than keeping track of when free flights had been earned. As the programs quickly matured, the airlines developed systems to track the flight histories of customers. The first uses were internal—to fine-tune routes and schedules, and to offer passengers discounts and other specials to try to shape travel behavior, first for the airlines and soon for their hotel, rental car, and restaurant partners.

Here's where it got creepy. I was traveling a great deal between Chicago and Silicon Valley, almost exclusively on United Airlines, which had the best schedules between Chicago and San Francisco. One day I received a letter from the manager of the Fairmont Hotel in San Francisco, where I had never stayed.

"Dear Mr. Downes," it read. "We know you travel frequently between Chicago and San Francisco, and we'd like to invite you to stay at the Fairmont on your next trip." The letter offered some discount or freebie.

Of course I knew that the letter had been generated by computer, using a simple extraction of United's Mileage Plus database for Chicago customers with frequent trips to San Francisco. The list may never have even been made available to the hotel, but more likely to a third-party mailing service, which actually produced and sent the letter. The manager didn't write the letter or sign it; he certainly never saw it. No human other than me likely did.

Knowing this didn't help. There was something about the letter that went over a line I didn't even know I had drawn. I didn't mind that United knew where I was going. And I didn't mind their giving my address (there was, of course, no email in those days) to their hotel marketing partners. I wasn't heading to San Francisco for any purpose about which I was embarrassed or which I needed to keep secret. But still, there was something disturbing about the manager of the hotel "knowing" my specific travel history and contacting me about it. Something I couldn't explain rationally.

During that period I was a member of the board of directors of the ACLU in Chicago, where I lived. So I understood that although the airline had crossed a line that offended me as a customer (and I let them know, for whatever that was worth), they had broken no law.

The situation, it's worth noting, would have been different if the same kind of data sharing had taken place between two branches of the U.S. government—say, for example, the Federal Aviation Administration and the Internal Revenue Service. Under the Privacy Act, federal agencies may not "disclose any record . . . to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains." Had the IRS used flight manifests from the FAA to target business expense audits, my reaction would have been considerably different. I would have sued.[61]

This suggests a further enhancement of the creepy factor equation. The degree of the emotional response we have to a novel use of personal information is often determined not so much by the use itself but by who is using it. The more distant the user is from one's immediate circle of intimates (friends and family), the more likely the new use will generate an uncomfortable emotional response. Or, to put it another way, the more unpredicted the use, the higher the creepy response. This suggests variable U for user:

$$P*U \rightarrow \frac{E}{F}$$

Or in English: the more personal the information, amplified by the degree of disconnect with its user, the more emotional the response to a novel use—but still diminishing over time with increasing familiarity.

The more unpredicted the use, the higher the creepy response.

That added variable highlights one of the most serious defects in what passes today for a public policy debate over privacy and how we should or should not surround it with legislation. Privacy is often a matter of context—information that seems perfectly natural for friends and family to have may have a higher creepy factor if it's being used by companies with whom one does business, even higher if it's being used by companies with whom one does not do business.

It's fine for you to know that today is my birthday, but if the grocery store somehow figures it out and sends me a special coupon, I'm going to flinch pretty hard. How did they know? What else do they know? Why do they care? Creepy.

The creepy factor goes up even more, at least in the United States, if the user is a government agency. And the most unwelcome form of information use is by criminals or for otherwise destructive purposes. If the information is being used to defraud me, or by a stalker or a bully, or to trick me into accepting viruses or malware on my computer to be passed along unknowingly to friends and family, there's no hint of a transaction with mutual benefit. Economists don't like transactions that don't add value to anyone. In law, we call them crimes.

Information use, let alone philosophical concepts such as "privacy," can't be regulated in the abstract. Aside from the problem of identifying what is and is not private (or even personally identifying), the use of the information has to be judged against the purpose of the user. Even within the broad categories of users suggested above—friends and family, familiar businesses, unfamiliar businesses—there are uses that are and are not acceptable that depend on context. If you're signing up for a free newsletter, there's no reason why a website would need to know your telephone or credit card number. (In fact, if they ask, it raises suspicions about the legitimacy of the site.)

Determining acceptable and unacceptable uses of information is often highly subjective.

But obviously if you are trying to buy something, it's understandable for a merchant to ask for that information, along with a shipping address. Likewise, questions about health are extraordinarily intimate, but how else to get diagnostic help from a medical service?

Consider Ancestry.com and other online genealogical services. These are companies who, without anyone asking and without anyone's permission, have collected vast databases of deeply personal histories that, if the service has done its job, cover just about everyone's family tree—bad seeds and all. Yet rather than complain about this multi-generational invasion of privacy, users pay for the privilege of using it. The service is only valuable if the company has done a good job of invading the user's privacy ahead of time—a service for which, in the genealogy context, the consumer is willing to pay.

As these examples suggest, determining acceptable and unacceptable uses is often highly subjective. There may of course be general categories of use that many people would agree to—or at least agree are unacceptable. No one would think it appropriate for Netflix to include questions about communicable diseases or digestive problems as part of account signup.

No matter—even if users don't think explicitly of the costs and benefits of giving up certain information in certain transactions, the creepy factor is always lurking in the back of their minds, a kind of binary switch that, if thrown, will click the magic "X" in the corner of the browser window and make the discomfort go away.

That's the problem with debating privacy legislation. We don't know and can't say *ex ante* which information that refers to us or our transactions is "personal" (in the emotional sense) or "private," nor can we say which uses of that information we'll find pedestrian and which we'll find invasive, and how long it will be before we get used to it. It is, after all, an emotional response, which makes rational discussion difficult if not futile.

For better or worse (almost certainly better), Internet users are hooked on the "free" software, content, and services that rely for revenue on information collection and use. So are the service providers. So we need to figure a way to head off a looming crisis of faith about what data is being collected and how it

is used—a crisis that goes under the unfortunate misnomer of "privacy" when it is really about economics and who gets to extract value from information. There are a few interesting proposals to consider—one not so good and the other much better.

A Bad Solution: Privacy as Property Ownership

Warren and Brandeis proposed to combat technological advances in data collection and distribution with a new enforceable right of privacy. But the plan failed. As legal innovation limped along, slowed in large part by latent or overt First Amendment concerns, technology galloped ahead. A similar fate seems likely for much of the current crop of proposed privacy protections. Even if they pass, they are likely to be so specific to particular uses and technologies ("pop-up ads," "spyware") that by the time they can be enforced they will have become anachronisms.[62]

So it's worth asking if there's a more efficient and effective way to resolve our conflicting views of information use—to quiet the internal struggle between Puritan and frontiersman. How, in other words, can we lubricate social interactions with accurate information without too often triggering the creepy factor's visceral response?

One possible solution is to remove emotion from the debate by characterizing personally identifiable information as a kind of personal property that individuals own, subject to market transactions for use and transfer. By turning information into property and assigning the initial ownership to the individual to whom the information refers, the idea goes, privacy would become just another form of "intellectual property" like patents and copyrights. The propertization of privacy is an old idea, going back at least to a 1993 article by Sheldon Richman.[63]

Support for the ownership of personally identifiable information comes from a wide range of legal scholars, including Lawrence Lessig, who summarized the arguments for and against this approach in an article that advocated for it.[64] Lessig argued that information use today is subject to the whims of those who collect it—too much so. Without property rights assigned in the first instance to those to whom information refers, it's difficult to characterize use of that information without permission or compensation as what he believes it really is: stealing. "If people see a resource as property, it will take a great deal of converting to convince them that companies like Amazon should be free to take it. Likewise, it will be hard for companies like Amazon to escape the label of thief."[65]

There is an obvious appeal to this approach. It takes privacy out of the realm of posturing and amped-up creepy-factor reactions and into an area of law and policy that is established and rational. The creation and management of property rights are as old as the oldest legal traditions in Western Europe. Treating intangible information as a kind of property and applying analogous principles to its ownership, use, and transfer is likewise deep-rooted, going back at least to 1710 and the Statute of Anne, which established copyright in England. There is tradition here, as well as precedent. There is also considerable understanding of both the effectiveness and limitations of such systems.

The property rights solution is elegant and logical: assign property rights to consumers for personally identifiable information, then give them the tools to manage and enforce those rights, including, if they like, to sell them. If a coalition of government agencies and responsible corporate users can get together and establish enforceable property rights over private information, anarchy will subside. Emotion disappears; problem solved.

Those arguing for the ownership of privacy are on the right track but for the choice of metaphor. It is certainly true that information can be thought of as a kind of property—initially assigned to one party, and then bought and sold through market transactions. But there are a few problems. Most consumers—indeed, most economists—only understand property in its tangible form, and have trouble applying

It's worth asking if there's a more efficient and effective way to resolve our conflicting views of information use.

It is certainly true that information can be thought of as a kind of property. But there are a few problems.

the very different economic principles that apply to intangible property, which includes all forms of information. Accounting for intangibles on corporate balance sheets, for example, is still in a primitive state of development, despite the increased importance of intangibles in determining corporate value.[66]

The explicit analogy between information ownership and the current state of copyright and patent law makes the problem messier. Over the last few decades, cynical and counterproductive extensions to the terms of copyright and mechanisms for enforcing it have poisoned consumers against any coherent understanding about what it would mean to "own" privacy rights or the like.[67]

Likewise, the increased generosity of patent offices, particularly in the areas of software and business methods, has bred a counterproductive culture of patent trolling, expensive litigation, and interference with innovation. Patents are no longer seen as a beneficial form of propertized information, even among companies who hold them and economically minded legal scholars.[68]

The general concept of "intellectual property" has been tainted, perhaps irredeemably so. Including "private" information under that heading would complicate more than it would clarify.

Another objection to the ownership approach is its unexplored assumption that the initial allocation of a property right should go to the individual to whom the information refers. That starting point isn't obvious. While the information we are talking about *refers to* or *describes* a particular person, that does not mean that the person actually exerted any effort to create the information, or that they have done anything to make it useful in combination with the information of other individuals. You spend money, accept credit, and pay your bills, but that doesn't mean you've done anything to make a useful record of your credit history future lenders can evaluate.

So we might instead think that those who unearth, normalize, store, and process information ought to be the initial owners of any property rights to it. For one thing, they need the economic incentive. Why else would a company go to the trouble of collecting various public and private records of your payment, employment, and asset history in order to create a credit profile? Under the view of Lessig and others, the moment that profile was of any value, its ownership would be assigned to the individual to whom it refers.

If that were the property rights system for privacy, no for-profit entity would bother to create credit profiles, which require not only an individual's information but the ability to compare it to the information of large groups of similar and dissimilar consumers. And unless you live your life paying cash for everything, you need someone to compile that history. Otherwise, there's no basis for a lender to determine the appropriate risk for a loan. Your lender will either make no loans or charge exorbitant interest rates. This is a central defect in Lessig's assumption and the less sophisticated claim by some privacy advocates that you "own" information simply because it refers to you.

Initial allocation can be crucial, and Lessig has picked the wrong starting point. We know this from the work of Nobel prize-winning economist Ronald Coase and the so-called "Coase Theorem." As Coase explained in a seminal 1960 essay, the initial assignment of a new property right will not matter if the market for trading the right is functioning without friction.[69] Since markets never function without friction, Coase concluded that the initial allocation of any property right should be the one that results in the least amount of avoidable overhead, or what Coase had earlier termed "transaction costs."[70]

In his famous example, he considered a new railroad that ran along the field of a farmer. The train engine gives off sparks as it passes, causing fires that damage the farmer's crop. Does the farmer have the right to be free of the sparks, or does the railroad, which operates under the transportation laws of the state, have the right to be free of liability?

For Coase, the question was not one of fairness or morality, but rather of which rule led to the most efficient use of resources for

society as a whole. Coase reached the startling conclusion that in a perfect market system, it wasn't necessary to decide who should have the initial allocation. If the farmer had the right to be free of sparks, the railroad would be willing to pay for the privilege of polluting an amount somewhat less than the value the railroad received for running additional trains, or running them at higher speeds and therefore causing more sparks. If that amount was greater than the damage to the crops, the right would change hands.

On the other hand, if the railroad began with a right to pollute, then the farmer would be willing to pay an amount somewhat less than the cost of the damage to his crops to have the railroad attach spark-arresting devices to the engines. If that amount was greater than the cost of the spark arresters, again, the right would change hands

These examples assume that there are only a few parties involved, and that there are no costs associated with negotiating, drafting agreements, and enforcing them—the transaction costs. That's where Lessig's approach gets into trouble. In Lessig's view, every individual should begin with a property right to all information that refers to them. If corporate users want it, they will have to negotiate a price for it. If the price is too low, consumers won't sell, and the information will remain private. If the right deal is reached, the information will be transferred, and will no longer be private.

But electronic information being collected today on the Internet and elsewhere involves billions of users and perhaps thousands of different data collectors. Up until now, the default practice, at least in the United States, is that transactional information (identifiable or not) can be collected unless the user opts out—either by selecting particular privacy options or by walking away from the interaction when a service starts asking for the wrong data. And that's fine, because most consumers are comfortable with the data being collected most of the time. (We know that because the Internet, unlike the rest of the economy, is still growing quickly, fueled by consumer information.) It also makes economic sense—it's the allocation that leads to the fewest transaction costs and therefore the least amount of overall social loss.

Flip the allocation around and the system comes to a crashing halt. If data can only be collected on the basis of a negotiated agreement with each individual consumer (and perhaps each individual data element), the transaction costs go through the roof. Indeed, for the most part those costs would be far greater than the value to either party of completing a trade. Transaction costs higher than the value of the transaction put an end to hopes for a market for any kind of property, private or otherwise.

That's the problem with simple-minded proposals (I don't include Lessig's proposal in that category) to "just" change the default rule on the Internet from opting out of information collection and instead to requiring each user to opt in with each data collector, or perhaps even with each specific use. If consumers want to be tracked, the proponents argue, then why not require them to say so explicitly?

The reason is that the effort to educate oneself on the pluses (free services) and minuses (a much smaller Internet) of participating, and determining the fair market value for information collected largely for future uses, would overwhelm most consumers. Far fewer interactions would take place, and those that did would take more time and effort by consumers. The transaction is roughly the same, but the transaction costs would be fatal.

No doubt there are some Internet users—true frontiersmen, perhaps, with little love of Puritan transparency—who would be willing to give up on ad-supported free services in exchange for complete anonymity. Such users would either have to pay directly for the services—search, email hosting, photo and video sharing, social networks, music and television programming—or go without them. They may even prefer that model to today's wide open Web.

But changing the default rule to allocate the initial right to decide the structure of the Internet would come at the cost of inconveniencing everyone else. We might make such a policy decision if we understood all the pros

Most consumers are comfortable with the data being collected most of the time.

If everyone had the right to forbid the use of any private fact, basic institutions, notably the press, simply couldn't operate.

and cons, but it's disingenuous to argue, as many privacy advocates do, that there's no real difference between the two approaches.[71]

Let me give a concrete example of the problem of transaction costs. Of the experiments in new privacy rights the common law courts engaged in after Warren and Brandeis's article, one is the "right of publicity." The right of publicity allows famous people to prohibit uses that they do not license of their likenesses, voices, or names in advertising. This is the only right that survives today with much force, especially in states such as California and New York with large, politically influential populations of celebrities.[72]

This rule isn't so much a right for the famous person to preserve their anonymity as it is to change the initial allocation of information-use rights. Rather than treating the name and recognizable likeness of a celebrity as public information, in other words, it requires an advertiser to negotiate for its use with the celebrity (or possibly the celebrity's heirs). And it applies only to use by an advertiser or other who wants to trade off the fame created by the celebrity's efforts. News sources can still name the celebrity, and anyone can still utter true facts about the celebrity.

The risk of a broader rule of privacy, one that applies to any historical or descriptive fact about any individual, is a problem of monopoly. If I allocate to the individual a property right to any fact that relates to or describes them, then I have only one possible party to bargain with for the use of that information. The risk is high that the individual will misjudge the value of their individual privacy and simply refuse any price. What would be otherwise economically valuable transactions won't occur, leading to what economists call "dead weight loss."

That monopoly problem doomed many of the new rights, including the torts of "false light" and "invasion of privacy," that some state courts tentatively embraced in the early 20th century. Judges quickly realized that if everyone had the right to forbid the use of any private fact, basic institutions, notably the press, simply couldn't operate.

Consider the example of Luther Haynes.[73] Haynes, far from a celebrity, was a sharecropper who moved to Chicago from Mississippi in the 1940s. There he married a woman named Ruby Daniels, but the marriage later fell apart due in part to Haynes's drinking, overspending, and neglectful parenting. The couple split up, and Daniels descended into poverty and the horrors of early 1960s public housing and other Great Society programs.

We know all this and quite a bit more about Haynes from *The Promised Land*, an acclaimed nonfiction book by Nicholas Lemann.[74] Though the book is principally an account of the migration of African Americans to the North, Lemann tells it through the example of Ruby Daniels, a dramatic story of the human costs that, Lemann suggests, were paid by millions like her.

The problem was that Daniels' privacy—which she willingly gave up to Lemann as part of his research—was in some sense the joint property of Haynes, who did not participate in the book. By the time *The Promised Land* was published in 1991, Haynes had cleaned up his act. He had stopped drinking, had remarried, and was a deacon in his church. He and his new wife were deeply embarrassed by the truthful but painful disclosures in the book, and he sued Lemann and his publisher in federal court, arguing that Illinois law (where Haynes lived) still recognized invasion of privacy.

Had the disclosures in *The Promised Land* involved public figures such as government officials, the First Amendment would have given Lemann wide berth to report them and would have protected him from liability even if he had gotten his facts wrong. So long as his investigation did not sink below the "actual malice" standard of *New York Times v. Sullivan*[75]—which held there can be no action for defamation unless the paper knew of the untruth or recklessly failed to investigate it—Lemann would have been immune from paying any damages.

Haynes was no public figure, but in any case the facts he complained about were true. So Haynes's principal legal claim was for in-

vasion of privacy. (Ironically, as with all legal cases claiming defamation or related privacy torts, bringing the lawsuit ensured more publicity of the private facts, and this time in freely quotable public records.)

Reviewing the history of that tort in Illinois, appellate judge Richard Posner concluded that the state had never fully embraced it. If it survived at all as an actionable offense, he wrote, invasion of privacy was limited to the disclosure of much more intimate facts than Lemann's book had described—perhaps the specifics of the couple's sexual practices. Haynes was out of luck.[76]

I was working as Judge Posner's law clerk when the appeal came before the court, and I confess that I felt deep sympathy for Haynes. After all, he didn't ask to be a figure in Lemann's book; he had achieved notoriety simply because Lemann's research had led him to Haynes's ex-wife. Haynes wanted the court to recognize what the Europeans might call his right to be forgotten, to have his early life erased so that his friends, family, and employers would judge him solely on his present conduct. Imagining embarrassing facts from my own youth, my response to Haynes' predicament was high on the creepy factor.

But difficult cases, as the saying goes, can make bad law. The problem with the right to privacy that Haynes wanted to enforce, as Posner correctly concluded, was that its cost to society was far more than the cost to Haynes's reconstructed reputation. Haynes was asking for monetary damages for his injury, but might have equally asked the court to forbid publication of the book until the publisher removed all references to him. As a monopoly holder of a property right to facts about his past, Haynes likely wouldn't have traded his right for any amount of money. That would have been the danger in allocating the right to him, and the reason Illinois courts, Posner concluded, would not do so.

Haynes, of course, was just one person, and Lemann's publisher could surely have afforded to pay the damages he requested. But had Haynes prevailed in his lawsuit, it would have signaled to authors of nonfiction books that they could not write about any individuals without their permission—permission many if not all individuals like Haynes would never grant.

Lemann needn't have written specifically about Haynes; he was just unlucky enough to have once been married to Ruby Daniels, a subject the author found compelling enough to anchor his narrative. But presumably everyone in similar circumstances described in the book would have also refused to sell a property right to privacy, had they had one. With the allocation of rights assigned to the person to whom information refers, nonfiction writers would be limited to writing in the abstract, or creating composite characters, exposing them to claims that their work wasn't concrete and therefore wasn't convincing.

It's also worth noting that the facts Haynes wanted to suppress were facts that also described the life of his ex-wife. Daniels, the victim both of Haynes and the welfare system, wanted her past exposed, not for purposes of retribution against Haynes but to have her deeply powerful struggle validated to Lemann's readers. When facts relate to information, even intimate information, about more than one person, how would a property right be allocated? Would it be shared property, owned equally by everyone referenced? If not, would any one person hold a veto, as Haynes argued he did, denying all the others the ability to sell, trade, or otherwise dispose of true facts as they wish?

Monopoly, joint ownership, and other transaction cost issues suggest that the more socially efficient initial allocation of a property right to private information should begin with the entity that collected the information in the first instance. But how then would the property right ever shift to the individual to whom the information refers? How, for example, could you "buy back" your credit information and take it out of circulation, assuming you wanted to do that?

In part, the answer is legislation that already reduces the transaction costs of managing some financial information between users and individuals. Under the Fair Credit

When facts relate to information about more than one person, how would a property right be allocated?

Reporting Act (FCRA), for example, consumer reporting agencies cannot collect certain information, including accurate but dated information. They must also correct errors—that is, inaccurate information, even if it is not personally identifiable information.[77] This is an example of the kind of information regulation that can work: (1) targeted to a specific kind of information, use, and user; (2) identifying clear consumer harms from inaccurate or negligent information collection; and (3) remedies that are both enforceable and directly responsive to the harms.[78]

Under the FCRA model, a market is created in which individuals can repurchase their financial reputations. To buy your way out of unpleasant but true negative financial facts—late payments, frequent changes in employment, and other risks relevant to future creditors—you need to invest in improving your reputation. That requires not a payment to the credit bureau but the discipline of practicing the kinds of financial responsibility that generate positive facts. Over time, these outweigh and replace the negative ones.

Let's take some other examples. What if I decide that the profile Amazon has compiled about me and my preferences has taken an uncomfortable turn, and the company is now suggesting or advertising to me products that I am interested in, but either wish I wasn't or am embarrassed to see revealed, even to me? Similarly, what happens when my choice of TV viewing trains my DVR to record suggested programming that I would rather not have suggested to me (in my case, too many cooking shows and superhero cartoons—accurate, but awkward)?

Here the process of buying back my privacy is cheap and simple. For Amazon, I can simply cancel my account and open a new one with a different user ID. (Amazon does not require me to provide authentication that I am a particular person, only that I am authorized to use whatever credit card I use to make purchases). It's even easier with my DVR. I just reinitialize the device and erase all the locally stored data that has been collected. (Likewise with cookies and other tracking tools for the Web.) I lose the usefulness of the services that work with that data, but I can easily retake control of the relationship and, in doing so, my privacy.

Transaction costs aside, the joint ownership of the facts Luther Haynes hoped to suppress raises a more fundamental problem with the property rights proposals of Lessig and others. When they speak of individuals being the initial owners of "their" information, just what information are we talking about? Lessig and others answer "personal information" or "private information." But these answers simply beg the question.[79]

Problems of definition in the property approach run deep.

Problems of definition in the property approach run deep. Is "my" information any information that I enter into some application; that is, information that I first translate to digital form? Or is it information that refers to me in an identifiable way, regardless of whether I had anything to do with its creation? Or only information that somehow defines an existential sense of self—information that refers to me in a deeply personal, intimate way? Are the addresses of websites I visit private information? The inventory of items I buy from you? The photos I take of members of my family?

Information "on" me, a Senate staffer said at a recent privacy conference, "is mine. It's not yours." Good rhetoric, but not much of a basis for defining property rights. Much of the information collected "on" me isn't private or even personally identifiable. It only has value when someone else goes to the trouble of codifying it, often without any effort from me.

FTC commissioner Julie Brill, perhaps recognizing the lack of interest most marketers have in individual data, includes in her definition of protectable information "not just the raw data, but also how the information has been analyzed to place the consumer into certain categories for marketing or other purposes." Her view of transparency is not just providing the consumer with access to "their" data, but also with the algorithms for processing it.[80]

There are problems with all three alternatives. The category of information I initiate or create is both under- and overinclusive. I in-

troduce all sorts of data into the cloud. While some of it is both personal and sensitive, much of it is utterly mundane—a review on Yelp, a bid on eBay, a click on a link on my Yahoo! homepage (recorded through a cookie) or a Google search result.

At the same time, much of the most personal information about me is entirely created by others, often using a great deal of private information that refers to other people. A credit score is a calculation that is based on data collected by credit card companies, banks, employers, and others and is only useful when it can be compared to the credit scores of others. (Is 680 a good score? I can't answer that without knowing the percentage of consumers that have higher and lower scores.) Would I own the credit score (and perhaps those of everyone else whose data was needed to create mine), even though someone else went to all the cost and trouble of preparing it? Would I own the list of all the links I clicked on? Neither? Both?

Falling back to the third alternative—information that is existentially private, that is, information that defines who I am—undoes the goal of propertizing privacy and taking it out of the realm of the abstract and illogical. For now I have left the world of neutral, unemotional property rights, bought and sold on the open market. Information that is private because it intimately and deeply defines who I am as a person is the least valuable and least likely to be legally exploited (blackmail is a crime). It is also the most subjective and the most contextual. I can't define it, to paraphrase Supreme Court Justice Potter Stewart in a famous case about obscenity, but I know it when I see it. We're right back to the creepy factor.

For most people, the contents of some if not most email to friends and family would almost certainly be categorized as private information. But what about more abstract data, such as the number of email messages I send in a particular period of time, or the route a certain message takes getting from sender to receiver, stripped of actual content or subject or even the identifier of the sender and receiver? Though these data may be associated with me in an identifiable way, most people would agree that there's nothing private about them. What is personal, it turns out, is in the eye of the beholder, or rather, in the eye of those who perceive me and use the information to identify and evaluate me.

We don't know what kinds of information Lessig and others have in mind when they propose that legislation should create a new property right and allocate its initial ownership to "you." That will make it difficult to satisfy the goal of privacy ownership in the first place—to create a market for buying and selling that right. Systems of property require certainty as to the kinds of rights associated with ownership.

In traditional property systems, such as real estate, certainty is reflected in the idea of holding "title," or proof of ownership. As anyone who has ever bought or sold a home, car, or other valuable piece of property knows, the cost simply to determine title (and in real estate, to insure against an incomplete title search) can be significant—again, likely more than the value of the transaction itself in the case of many less-significant information exchanges.

This brings up a more serious drawback to the property rights solution. In real estate, as in personal property, there is also certainty as to the thing to which the right attaches (the "res" in legal terminology). I either do or do not have title to my house and land, but what constitutes the house and what constitutes the land can be easily determined. For the house, a visual inspection is all it takes. For the land, a visit to the county records office, where the metes and bounds of the parcel is defined and the chain of title recorded.

Information is different in a significant way. We can't see data; we can't hold it in our hands. To say that I own my data doesn't mean the same thing as saying I own my car. If it is data about me that was created by a company or government entity, I may never even know that it exists. The data is likely stored in multiple copies and formats in the cloud. Each copy is identical and equal in value to every other copy. There is no scrap or salvage value to information.

To say that I own my data doesn't mean the same thing as saying I own my car.

The more a piece of data is used the more valuable it becomes.

Information, as noted earlier, belongs to a very different category of goods and services that economists refer to as intangibles. Trademarks are intangibles. So are patents. The goodwill of an ongoing business, from an accounting standpoint, is an intangible, and so is peace of mind. (We're certainly willing to pay for it.) All information, private and otherwise, is intangible.

Under the law, intangibles can and often are treated as a kind of property, and in many cases they have been for decades. The problem with applying property rights to information is that intangibles have different and often counterintuitive economic characteristics from tangible property. Unlike physical goods, for example, intangible property can't be easily controlled by the owner. It is "non-excludable," to use the economic term.

Information, Stewart Brand famously said, wants to be free. Brand meant free in the sense of not costing anything, given the trajectory of Moore's Law.[81] But information also wants to be free in the sense of being unhindered in its migration to use that is economically valuable. In either case (or both), once information takes a digital form, it is very hard to control who uses it, or to enforce a system of payment for its use, even one with criminal sanctions. Just ask any copyright holder.

Digital information also differs from tangible goods in that it can be duplicated into an infinite number of identical copies at little to no cost, allowing consumption by additional users. In most cases the duplication doesn't reduce its value. Economists refer to that feature of information as "non-rivalrous."

The more a piece of data is used the more valuable it becomes, like a television program or a novel, or the nonproprietary, open standards that define the Internet itself. We can all use it, manipulate it, and remix it, all at the same time. The more it is used, the more popular it becomes, and that popularity can often be monetized. This property is what economists call "network effects."

When we're done, the information, unlike a barrel of oil, is still there, perhaps more valuable for having been used. The Internet's protocols weren't worth much when only a few government and academic computers made use of them. Now that billions of devices rely on them every nanosecond, their value is incalculable. And yet no one pays anyone else for their use, at least not directly.

That's not irony. It's just a very smart decision to eliminate the transaction costs of charging for use of the standards in order to maximize network effects. As a result, users build something much more valuable on top of them. Indeed, it's the main reason the Internet protocols (IP) became today's dominant network standard, rather than more sophisticated but proprietary alternatives offered until very recently by leading computing and communications companies. Every company whose profits rely on the existence of the Internet is, at least in part, monetizing the value of the standard.

Information is non-excludable and non-rivalrous—the opposite of tangible property. It is difficult for economists, let alone consumers, to keep in mind the different economic principles that apply. That makes creating a new market for property rights to private information, if nothing else, a difficult problem in norm generation. We'd have to teach consumers that there are two kinds of property, and which of their possessions fall into which category.

If the upside-down economic properties of intangibles wasn't hard enough for users to understand, there is the added problem, noted earlier, that the idea of information as property has been tainted by misuse of a set of laws that grant special property rights to creative information—by which I mean trademarks, patents, trade secrets and, worst of all, copyrights. This group of laws is often referred to as "intellectual property," a term that has been used intentionally to confuse users into believing that protected information is not intangible but is literally somehow a kind of physical property, whose unauthorized copying constitutes "theft" or "piracy."

Before the digital age, the intangible features of intellectual property, especially copyrighted works, didn't much affect their

economic or legal treatment. That's because creative works couldn't be experienced without first translating them to a physical medium—a book, an 8-track tape, or a canister of film. We experienced the information only through possession of a physical copy and specialized devices that "played" it.

Information embedded into media couldn't be "free" in either sense of the word, which made it easier to control but more expensive to distribute. The costs of the media were so significant, in fact, that they have long been the dominant characteristic of creative enterprises. Journalists don't work for information services, they work for newspapers. Songs were available not in music stores but in record stores. The whole industry defined itself with reference to the physical copies—it wasn't creative information; it was "mass media." "The medium," as Marshall McLuhan cryptically said, "is the message."[82] The costs of creating and distributing content so dominated the supply chain, in other words, that the creative part often didn't seem especially important to those in the industry.

When copies had to be made in physical form, the economics of tangible goods dominated. You owned a physical copy of a movie, but you didn't own any rights to the movie itself—you couldn't adapt it for another medium, you couldn't produce a sequel, and most of all you couldn't make and sell additional physical copies.

The migration of information products from physical copies to digital distribution has, at least in theory, made it easier to think of copyrighted works in particular as intangible property. But producers, distributors, and retailers of physical media confused consumers by promoting the idea that owning a (decaying, fragile, and soon-to-be-obsolete) copy was equivalent to owning the underlying, intangible content. (How else to convince consumers to replace one generation of media with the next one?)

At the same time, advertising-supported content made it possible to deliver music on the radio and programming on television to be free of charge over the public airwaves. "Free" content underscored the idea that the only information that was valuable was information that could be held in some media product. The result: a generation or more of consumers who simply can't understand that information really is intangible.

Media and software companies, who themselves may not be so clear on the concept of intangibles, have made things worse with their long-standing campaigns to criminalize unauthorized reproductions. That was another side-effect of Moore's Law. When content required physical media, unauthorized copying was expensive and easy to uncover. You needed industrial equipment to make the copies, a distribution network to get them to market, and access to retail channels to sell them. Each of these steps, to be successful, exposed the unauthorized copier to discovery and the application of both civil and criminal sanctions.

The digital revolution, however, removed nearly all of the costs of copying and simultaneously created virtual manufacturing, distribution, and retail outlets that were superior[83] and, at least with early examples such as Napster and Grokster, largely untraceable. To put it mildly, the content industries freaked out. The Recording Industry Association of America went so far as to sue their own customers. None of them could have paid the statutory fines, and few understood that what they were doing was any different from listening to the radio.[84] The strategy neither slowed the unauthorized reproduction of musical compositions nor collected significant damages for technical violations of U.S. copyright law.[85]

All that the RIAA's lawsuits (and those more recently by the film industry) have done is create a new language that paints any effort to tap the astonishing potential of digital distribution as both a sin and a crime. Services that help users find torrented content are "rogue" websites "trafficking" in "pirated" copies. Users who listen to songs without paying for them, or who try to listen to songs they have paid for in a different medium, are "thieves" "stealing" content. Unlocking devices or programs to remove limitations on their use are said to be "jailbreaking."

When content required physical media, unauthorized copying was expensive and easy to uncover. The digital revolution removed nearly all of the costs of copying.

Licensing has proven to be a much more flexible legal and economic system for dealing with intangibles.

Whatever one thinks of these efforts to police information use, this is the language of tangible, not intangible, property. When it comes to information, however, it's the language we're stuck with, at least for now. Applying the property metaphor to personal information would invariably bring with it a lot of intellectual property's unintended and dangerous baggage—baggage packed for us by the content industries.

The linguistic mess of IP law has already infected the privacy debate. Some users are adamant that they "own their own information," as if they had a natural right to go into every data center in the world and collect a piece of magnetic medium which had somehow been stolen from them by evil corporate pirates. It makes as little sense in the context of personal information as it does in the world of copyrights (where the piracy runs the other way). The metaphor, for better or worse, has been thoroughly corrupted.

Perhaps it will be rehabilitated as we move to a truly digital economy, where physical media is relegated to the world of nostalgia and collectibles. Ownership of copies will give way as the metaphor of content experience to rental, leasing, or use-based pricing.[86] (Think of the success Apple has had with iTunes and, more recently, the iCloud—"the new way to store and access your content.")

Or perhaps we'll continue to get most everything we value for free in exchange for various old and new forms of advertising, some contextual; some product placement; some, well, who knows what the future of advertising will bring? That is, assuming we don't strangle it in its cradle with panicked legislation.

A Better Solution: Licensing Personal Information

The privacy-as-property metaphor is a bad way to transform the property debate from the emotional excesses of the creepy factor into something rational and therefore actually debatable. But there's still hope. For the ownership model isn't that far from something that could prove useful. While intangible property can't be "owned" or "stolen," it can be licensed for particular and limited uses. Personal information, in other words, could be traded in markets that deal not in transfers of ownership but in licenses for use, including leases, rentals, and barters.

Though property and licensing are closely related, licensing has proven to be a much more flexible legal and economic system for dealing with intangibles. When you buy a ticket to a movie theater or a ski lift ticket, the seller isn't transferring ownership of the seat or the gondola, or even a partial or shared transfer of title. You're acquiring a right to use someone else's property, under terms and conditions specified in tiny type but more than likely established by custom and the desire of both parties to have an ongoing, mutually beneficial relationship.

The main advantage of a licensing model is that, unlike the transfer of property rights, there's no need for the transaction to specifically identify the property or to ensure the chain of legal title to it. There's no need to transfer possession of something that, in the case of information, can't be possessed. Licensing is simply permission to use, as general or as specific as the parties decide. The existential nature of the thing being used needn't be determined for licensing to work.

Licensing is the perfect model for information transactions, and it has already been used successfully for many different kinds of information products and services. Your cable provider doesn't own the shows it distributes. Rather, it licenses programming from producers and in turn licenses it to you to watch on authorized devices. Software has moved almost entirely away from the "purchase" of copies of programs on a set of disks to a license to download and execute, or, in the cloud, simply a license to use.[87] Software from Google and other Web-based service providers has always been available to users on a licensed basis, even though the user in most cases pays for the license not with cash but with agreements to share and receive information.

Even when you buy physical copies of information products, you aren't buying the information. Paying for that boxed set of *The Lord of the Rings* movies on extended edition blu-rays, for example, actually encompasses two very different transactions. You own the box, the enclosures, and the DVDs themselves, but you only license the data contained on the disks. The license can be limited (no public showings) or even terminated (watch for 30 days only), which may sound unfair from a property mindset but actually makes possible a wide range of different kinds of transactions, each priced accordingly.

Owners of Amazon Kindles may still talk of "buying" copies of the books they want to read, but the content is mostly in the cloud, available on demand through the Internet. So the terminology is wrong—Kindle readers are actually licensing the future right to read the book. They are paying for permission to use information, not to own or even possess a copy of it.

Proprietary databases, including those from Lexis, West, BNA, and other publishers, are also offered on use-based terms—so much time, or so many users, or both. And more and more application software—whether large corporate systems such as Salesforce.com or the billions of apps downloaded to smartphones and pad computers—is made available on a purely licensed basis.

That transformation, made possible by the Internet, is a boon to consumers. As Kevin Kelly argued in an influential 2009 essay, licensing information use is superior to owning copies of physical media. Physical media takes up space, gets lost, decays or can be damaged. Newer formats often improve on storage capacity, fidelity, and other features and functions.

> There are fewer and fewer reasons to own, or even possess anything. Via [the Internet], the most ordinary citizen can get hold of a good or service as fast as possessing it. The quality of the good is equal to what you can own, and in some cases getting hold of it may be faster than finding it on your own, in your own "basement."[88]

If only we can get past our 20th century prejudice of judging personal worth on the basis of accumulated wealth ("having the most toys"), we can experience the liberation of instant access to the entire corpus of music, film, literature, and services at our fingertips. Licensing rather than possessing copies also means we don't have to store it, clean it, maintain it, or update it when newer and better forms of storage or playback are developed. We might be on our way to information Valhalla. As Kelly says, "Access is so superior to ownership, or possession, that it will drive the emerging intangible economy."[89]

That, in any case, is one possible future for creative content. "Our" "personal" information is evolving to follow the same model, with the dynamics largely reversed. Instead of leasing information from providers, users are increasingly licensing information to them—demographic, transactional, preferences, intimate—in exchange for some kind of valuable service. In the market for personal information, it could be that truly valuable data is exchanged for cash (or coupons), but more likely we'll continue our wildly successful barter system, where information is exchanged for other information—for access to information services that are optimized and customized to our needs and preferences.

How does that market work? The key is the potential of network effects. Remember that intangible goods are different from their physical counterparts in that recombination and reuse make them more valuable rather than using them up. Your personal information may be valuable to you in some abstract sense, but it's really only valuable to others when it can be combined, compared, and repackaged with similar information from other providers.

My purchase history is interesting to my credit card bank because they can use it to figure out what other stuff I might want to buy and what it will take to get me to buy it. But it's really only useful as a network good when it

Your personal information may be valuable to you in some abstract sense, but it's really only valuable to others when it can be combined, compared, and repackaged.

can be combined with the preferences and history of like-minded purchasers. Then it can be used as bargaining leverage with sellers to get volume discounts or to convince them they're making the wrong stuff, in the wrong place, at the wrong price, or at the wrong times.

Purchase information also becomes more valuable, perhaps by orders of magnitude, when transaction information can be combined with information about my experience of the transaction. Did I like the product? How quickly did I use it? What did I use it with? Why did I throw it away? What features actually mattered in my decision to buy, and did those features turn out to be the ones I valued? That kind of post-transaction, subjective, and indeed private information (most of it is currently stuck in my head) can't be easily collected without my cooperation. And that gives me bargaining leverage—an information advantage.

In the past, you have likely used supermarket and other loyalty cards, which trade specific purchase data of a specific customer at a specific store and time for targeted discounts. That's a great example of mutually beneficial information licensing in action. It doesn't matter who "owned" the information, or even whether possessions changed hands. It was a joint creation in which one of the creators (the consumer) authorized the other (the store) to make specified uses of new information.

Let me give two other examples of this barter system now in use. One is the new idea of social shopping, where companies including Groupon and LivingSocial combine the buying preferences of multiple users in a local market. The combined preference information is used to convince a local provider of goods or services that there are new customers who could be acquired if only the right introductory offer is made at the right price and time. If enough users agree to eat at the new sushi restaurant, then it's worthwhile for the sushi restaurant to give us all a healthy discount on a meal, in hopes that many of us will make return visits at full price.

The offline version of that relationship includes buying groups such as Costco and Sam's Club. Members pay an annual fee—the price for the organizer to run the club. The more members, the easier it is to extract high-volume discounts from manufacturers. The more consumers the club can sign up, in other words, the more transactional information the organizers can collect, which they employ as leverage with manufacturers. That's the same kind of network effect that makes the Internet more useful as more people take advantage of it.

To reach the members of the club, in turn, the manufacturers produce special versions of their products (usually the regular products in larger-sized containers, which are cheaper to distribute) and sell them directly to the buying club. The manufacturers avoid several layers of middlemen (so do the buyers), and the extra-large sizes helps allay the complaints of traditional retailers of pricing advantage to the club. In this sense, Costco isn't a store at all; it's a consumer advocacy group, driving hard bargains on behalf of its members. (Priceline works on a similar model.)

The information we give up to participate in these kinds of information barters isn't especially personal, or at least wouldn't be considered so by most users. But what about truly private data? Social networks have already licensed our photos, posts, emails, and other personal content for limited use, mostly to target relevant ads and to help them encourage our friends and family to sign up too.

For the most part, this intimate data isn't being mined all that specifically, at least not so far. Perhaps the providers of these services understand the creepy factor and know that alienating users reverses the value of network effects, which, for social networks, is the beginning of a death spiral. (Just ask the operators of Friendster, MySpace, and other failed social networks. Once networks of any kind stop growing, they quickly begin to shrink.)

The inventory of useful information is about to experience an enormous expansion.

The inventory of useful information, however, is about to experience an enormous expansion, adding leverage for consumers in the information licensing market. Moore's Law, again, is the driver. Now that governments, businesses, and individuals are all on the In-

ternet, we're on the verge of moving to the next level of granularity. It's now cost-effective not just for individuals to have multiple computing devices, but for all the things we interact with to have connectivity as well.

This "Internet of things" will introduce modest processing, storage, and communications technology into each of over a trillion items in commercial use, allowing them to collect and transmit basic information about where they are and what they're doing. Our phones and other mobile devices, including cars, already participate in the Internet of things. Soon it will be appliances, furniture, livestock, light bulbs, fruits and vegetables, and pills.

How does the Internet of things work? In the archetypal example, a radio frequency ID tag is printed onto the packaging of each item—for example, a quart of milk). The tag transmits information about itself whenever it comes near a reader, sometimes operating on static electricity as the power source. The tag helps the store keep track of its inventory and impending expiration dates, and allows you to check out simply by walking past a reader at the exit. Once you're home, the milk, perhaps using the refrigerator as its server, can keep track of usage history and spoilage, letting you know when it's time to restock.

If we allow it, the milk can also pass its status updates (nanotweets?) up the supply chain, giving producers, distributors, retailers, and inspectors consolidated data of tremendous value. Instead of guessing at supply and demand, we'd actually know it. Manufacturing, marketing, pricing and promotion, product design, inventory control, and pretty much every other feature of the industrial economy would become far more efficient—in some cases, for the first time, genuinely scientific.[90]

This coming revolution underscores a feature of privacy that nearly everyone in the discussion today underestimates: The truly valuable uses of information in the future cannot be realized without deep cooperation and collaboration with users. A bank can collect transaction information and public records and create a credit score, but a bank cannot determine how you value your money without your participation. Product marketers can hold focus groups and conduct surveys to determine what to sell and when, but the sample sizes are tiny and unreliable compared to getting actual information from all their customers.

Power is shifting increasingly to users, who will use their digital networks—their social networks, their buying clubs, their email lists, the networks of their possessions—to negotiate for themselves the best possible price for the licensing of information. The need for consumer cooperation and collaboration in future information uses is the best hope for a nonlegislative solution to the privacy problem.

And not just an individual consumer. Nearly all these future information uses are valuable only in large volumes—collecting similar data from everyone. It only matters how well you like a particular product if the retail supply chain can aggregate that information with many other users. That's because intimate information is idiosyncratic, and not highly valued on its own. It is of little interest to any information user except those whose purpose is entirely destructive (e.g., blackmail). In that sense "private" information may come to be defined as information for which there is no market. It's worthless to anyone but the one person who values it exorbitantly.

The expanding market for information licensing, then, may solve the privacy crisis on its own, no new regulation or legislation required. Which is not to say the existing market for information licensing is working perfectly. There are many ways it needs to be improved. Here are some of the most pressing:

1. *Embrace meaningful disclosure*—Service providers must make as clear as possible what information is being collected and what they do with it. This doesn't mean more laws calling for "notice" or "transparency," which generally lead to volumes of disclosures so detailed and technical that any actual important information gets lost. Even a simple mortgage refinance includes over a hundred pages of densely worded disclosures mandated by perhaps a dozen different

The need for consumer cooperation and collaboration in future information uses is the best hope for a nonlegislative solution to the privacy problem.

federal, state, and local agencies. There may be some important information hiding in that mess, but absolutely no one is going to read it all. The more detailed the notice, the less likely it is to communicate anything. Useful disclosures would be short and to the point.[91]

2. *Simplify negotiations*—The higher the transaction costs, the lower the chances of a functioning, efficient market. That's especially true where there are potentially millions of participants and billions of low-value transactions going on all the time. Rather than encouraging information users to negotiate each data element individually (the so-called "opt in" model that some advocates propose, even for social networks whose purpose is to share personal information), look for ways to make it easy for users to vote yes or no on the entire slate of data, at least as the default. Similarly, user agreements, which can establish the basic terms for most information exchanges as an ongoing relationship, must be written to be read and understood by someone other than corporate lawyers.
3. *Secure the information*—Information is valuable, so treat it accordingly. Criminals and other destructive users are ramping up their efforts to gain access to and exploit all kinds of information. Governments, businesses, and consumers must each make better use of existing security procedures and technologies, including encryption, anti-malware, and physical security for data centers and devices. Business information users in particular should take seriously the risk that failure to embrace secure information practices, such as the ISO 27000 series of standards, will surely lead to legislative imperatives that will cost more and protect less. Security breaches are often the only reasons regulators can specify in the rush to enact new privacy laws, though the proposed laws rarely have anything to do with improving security.
4. *Improve self-regulatory practices*—For-profit and not-for-profit entities are emerging to validate the information-handling practices of business users. Businesses should support and embrace these initiatives and take seriously the need to display seals of approval and other indicia of compliance. At the same time, self-regulatory organizations must set real standards and enforce them. Consumers should be educated not to engage in information exchanges with users who don't comply with standards.
5. *Avoid crisis-management regulation*—Regulators must resist the siren call of the privacy crisis du jour, littering the law books with specialized statutes aimed at solving short-term technical problems that will have evolved or mutated before the ink is dry. Limited government resources would be better used to enhance public education on information licensing and to teach consumers how to be effective negotiators. Governments should encourage self-regulation on security, disclosure, and other important elements of the information licensing market, and make clear that fair bargains fairly entered into will be enforced, if necessary, through judicial processes.

Most issues of appropriate use and appropriate compensation for consumer information can and will be worked out by the parties.

These problems are both minor and manageable. The best thing that can be said for the licensing model for information—private or otherwise—is that it's already in place and functioning efficiently and effectively. No new laws must be written to create new rights, and no new regulators are necessary to police them. Abuses are likely to come from activities that are already criminal (hacking and identity theft) or from the government itself.

If current practice is any indicator, most issues of appropriate use and appropriate compensation for consumer information can and will be worked out by the parties. Consumers will continue to show more confidence and ability to express their collective will. If we can just control our reactions to the creepy factor and resist the temptation to

call in our industrial-era government regulators, the long-running and unproductive debate over privacy will be replaced by a more concrete conversation about propriety. That is, how will the wealth generated by valuable new uses of data—personal or otherwise—be shared among information producers and information users?

The legal framework needed for that conversation is already in place. We just have to catch up to our technological innovations. We need to evolve from emotional responses to data use to rational decisionmaking. And we need to do it soon.

Notes

1. See http://www.privacyidentityinnovation.com/.

2. Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," March 2012, p. i, www.ftc.gov/os/2010/12/101201privacyreport.pdf.

3. Ibid., pp. 22–38.

4. Ibid, p. i.

5. Al Franken, Senate Judiciary Subcommittee Hearing on Protecting Mobile Privacy, opening statement, May 10, 2011, http://www.franken.senate.gov/?p=hot_topic&id=1496.

6. Ibid.

7. According to Rackspace, the cost of a gigabyte of storage plummeted from nearly $20 in 2001 to only six cents by 2010. As technology costs decline, new cloud-based services are offering free or extremely cheap virtual storage services for individuals and corporate users, making their money on supplemental services. In 2011 alone, 1.8 zettabytes of new data were created, and projections are that the number of data storage servers will grow 10 times over the next decade. See "Decade of Storage from USB to Cloud Storage," *Rackspace.com* (blog), http://www.rackspace.com/blog/decade-of-storage-from-usb-to-cloud/; and Lucas Mearian, "World Data Will Grow by 50X in next Decade, IDC Study Predicts," *Computerworld*, June 28, 2011, http://www.computerworld.com/s/article/9217988/World_s_data_will_grow_by_50X _in_next_decade_IDC_study_predicts.

8. "200 Million Tweets Per Day," Twitter Blog (June 30, 2011), http://blog.twitter.com/2011/06/200-million-tweets-per-day.html.

9. Facebook, "Statistics," http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

10. In 2004, for example, the Electronic Privacy Information Center (EPIC), Privacy Rights Clearinghouse, and the World Privacy Forum sought to have Gmail declared a violation of California wiretapping law. Letter to California Attorney General Bill Lockyer, May 3, 2004, http://epic.org/privacy/gmail/agltr5.3.04.html. At a July 2012 conference, EPIC's executive director confirmed he continued to believe Gmail should be banned. See Berin Szoka, "Video of the Great Privacy Debate Now Available," August 7, 2012, http://techfreedom.org/blog/2012/08/07/video-great-privacy-debate-now-available.

11. "Do Not Track," described as some kind of functional equivalent to telephone "Do Not Call" lists, was a key recommendation in Federal Trade Commission, p. v, 3–4, 13, 28. Details are sketchy, however, as to what exactly is meant by "tracking."

12. Internet Advertising Bureau, "Internet Ad Revenues Hit $31 Billion in 2011, Historic High up 22% over 2010 Record-Breaking Numbers," April 18, 2012, http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-041812; Adam Thierer, "Birth of the Privacy Tax," *Forbes*, April 4, 2011, http://www.forbes.com/2011/04/02/privacy-tax-social-networking-advertising-opinions-contributors-adam-thierer.html.

13. Google 2012 Financial Tables, http://investor.google.com/financial/tables.html.

14. Lisa Stauber, "A Brief History of Television Advertising," *Television Blend*, Oct. 16, 2006, http://www.cinemablend.com/television/A-Brief-History-of-TV-Advertising-1298.html; Adam Thierer, "We All Hate Advertising, but We Can't Live Without It," *Forbes*, May 13, 2012, http://www.forbes.com/sites/adamthierer/2012/05/13/we-all-hate-advertising-but-we-cant-live-without-it/.

15. We're speaking here of traditional cookies. Flash or "supercookies" are more complicated. See "Cookie Respawning, History Case Dropped," *The Register*, Aug 22, 2011, http://www.theregister.co.uk/2011/08/22/privacy_charge_dropped_against_cookie_trackers/.

16. See Howard Beales, "The Value of Behavioral Targeting," 2010, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf. According to Beales's empirical study, conversion rates for behaviorally targeted ads are double the rates for general ads (p. 4).

17. "Half the money I spend on advertising is wasted; the trouble is I don't know which half." At-

tributed to John Wanamaker, see http://www.quotationspage.com/quote/1992.html.

18. See Larry Popelka, "For Successful Innovation, Sell Imperfect Products," *Bloomberg BusinessWeek*, January 25, 2012, http://www.businessweek.com/innovation/for-successful-innovation-sell-imperfect-products-01252012.html.

19. Arthur C. Clarke, *Profiles of the Future: An Inquiry into the Limits of the Possible* (New York: Harper and Row, 1962).

20. Larry Downes, "Privacy Panic Debate: Whose Data Is It, Anyway?", *CNET News.com*, April 27, 2011, http://news.cnet.com/8301-13578_3-20057682-38.html?tag=mncol;1n.

21. See "Geotracking Controversy Homes in on iPhone," *CNET News.com*, July 14, 2011, http://news.cnet.com/8301-13579_3-20057175-37/geotracking-controversy-homes-in-on-iphone-roundup/.

22. Tanzina Vega, "Congress Hears from Apple and Google on Privacy," *New York Times*, May 10, 2011, http://mediadecoder.blogs.nytimes.com/2011/05/10/congress-hears-from-apple-and-google-on-privacy/.

23. "Are your Gadgets Spying on You?" *NPR Science Friday*, May 6, 2011, http://www.npr.org/2011/05/06/136057336/are-your-gadgets-spying-on-you.

24. Brian X. Chen, "U.S. Senator Demands Privacy Policies for Smartphone Apps," *Wired*, May 27, 2011, http://www.wired.com/business/2011/05/u-s-senator-demands-privacy-policies-for-smartphone-apps/.

25. Marguerite Reardon, "Apple: We'll Fix iPhone Tracking 'Bug,'" *CNET News.com*, April 27, 2011, http://news.cnet.com/8301-30686_3-20057815-266.html.

26. "Apple Q&A on Location Data," Apple Press Info, April 27, 2011, http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html.

27. Ibid.

28. "Are Your Gadgets Spying on You?" *NPR Science Friday.*

29. Ibid.

30. William A. Niskanen Jr., *Bureaucracy Public Economics*, 2nd ed. (Northampton, MA: Edward Elgar, 1996).

31. Since 1996, for example, the FCC has expanded its requirement that mobile phones automatically provide location information to emergency service providers. See "In the Matter of Amending the Definition of Interconnected VoIP," Notice of Proposed Rulemaking, FCC 11-107 (2011), http://www.fcc.gov/document/amending-definition-interconnected-voip-service-section-93-commissions-rules-wireless-e911-.

32. See Kim Hart, "Yahoo Changes Data-Retention Policy," *Washington Post*, December 17, 2008; Chloe Albanesius, "AT&T Considering Its Behavioral Advertising Options," *PCmag.com*, August 14, 2008, http://www.pcmag.com/article2/0,2817,2328070,00.asp.

33. See John Eggerton, "House Judiciary Debates Data Retention Bill," *Multichannel News,* July 27, 2011, http://www.multichannel.com/article/471608-House_Judiciary_Debates_Data_Retention_Bill.php. The bill's title suggests retained data could only be used to investigate child pornography, but in fact any crime will do. See Mark Stanley, "How the Data Retention Bill Impacts You," Center for Democracy and Technology, February 27, 2012, https://www.cdt.org/blogs/mark-stanley/2702how-data-retention-bill-impacts-you-%E2%80%93-and-what-you-can-do-about-it; H.R. 1981, "Protecting Children from Online Pornographers Act of 2011," 112th Cong. http://www.govtrack.us/congress/bills/112/hr1981/text.

34. Hart.

35. Amy Lee, "Yahoo Extends Data Retention from 90 Days to 18 Months," *Huffington Post*, April 18, 2011, http://www.huffingtonpost.com/2011/04/18/yahoo-data-retention_n_850373.html.

36. See Henry D. and Frances T. McCallum, *The Wire That Fenced the West* (Norman, OK: University of Oklahoma Press, 1965).

37. Leonard J. Arrington, *The Great Basin Kingdom* (Cambridge: Harvard University Press, 1958).

38. Nathaniel Hawthorne, *The Scarlet Letter* (Boston: Ticknor, Reed, and Fields, 1850).

39. Arrington.

40. Frederick Jackson Turner, "The Significance of the Frontier in American History," in *The Frontier in American History* (New York: Holt, 1920).

41. Jim Harper refers to this as "practical obscurity." See Jim Harper, *Identity Crisis: How Identification Is Overused and Misunderstood* (Washington: Cato Institute, 2006), pp. 158–75.

42. Steven D. Levitt and Stephen J. Dubner, *Super-*

freakonomics (New York: William Morrow, 2011), pp. 139–190.

43. Joseph Heller, *Something Happened* (New York: Alfred A. Knopf, 1974), pp. 13–14.

44. Max Weber, *The Protestant Ethic and the Spirit of Capitalism* (New York: Scribner's, 1958). Weber argued that the "this-worldly asceticism" of Puritanism, encapsulated in the concept of a "calling," drove the development of capitalism and entrepreneurship in Western civilization.

45. European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union," COM(2010) 609 (2010). See Larry Downes, "My Own Private Memory Hole," *CNET News.com*, November 16, 2010, http://news.cnet.com/8301-13578_3-20022977-38.html; "US Lobbyists Face Off with EU on Data Privacy Proposal," *Spiegel Online*, October 17, 2012, http://www.spiegel.de/international/business/us-government-and-internet-giants-battle-eu-over-data-privacy-proposal-a-861773.html.

46. U.S. Const. amend. IV.

47. U.S. Const. amend. I.

48. See generally Allison Cerra and Christina James, "Identity Shift" (Cleveland: Wiley, 2012). There is also mounting evidence casting doubt on the value of many of the surveys conducted or financed by self-styled consumer advocates. See Daniel Castro, "New Survey Shows Some Privacy Scholars Lack Objectivity," The Innovation Files, Oct. 14, 2012, http://www.innovationfiles.org/new-survey-shows-some-privacy-scholars-lack-objectivity/.

49. Warren and Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 193 (1890). ("Of the desirability—indeed of the necessity—of some such protection, there can, it is believed, be no doubt. The press is overstepping in every direction the obvious bounds of propriety and of decency.") Warren, married to the daughter of a U.S. Senator, was motivated in part by outrage when trivial details of a social function attended by his daughter were mentioned in the *Washington Post*. Like today's social networks, photography came with both costs and benefits to social and family life.

50. For the development and decline of common law privacy torts, see *Haynes v. Knopf*, 8 F3d. 1222 (7th Cir. 1993) (Posner).

51. Warren and Brandeis.

52. Federal Trade Commission, p. vi.

53. Sean Ludwig, "LinkedIn Removes Photos from 'Social Ads' after Complaints," VentureBeat, August 11, 2011, http://venturebeat.com/2011/08/11/linkedin-social-ads-pictures-removed/.

54. Ryan Roslansky, LinkedIn Blog, August 11, 2011, http://blog.linkedin.com/2011/08/11/social- ads-update/.

55. Eric Goldman, "Big Problems in California's New Law Restricting Employers' Access to Employees' Online Accounts," *Forbes.com*, September 28, 2012, http://www.forbes.com/sites/ericgoldman/2012/09/28/big-problems-in-californias-new-law-restricting-employers-access-to-employees-online-accounts/.

56. See http://online.wsj.com/public/page/what-they-know-digital-privacy.html. The *New York Times* is also getting into the fear-mongering business. See Natasha Singer, "Consumer Data, but Not for Consumers," *New York Times*, July 21, 2012, http://www.nytimes.com/2012/07/22/business/acxiom-consumer-data-often-unavailable-to-consumers.html?pagewanted=all; Natasha Singer, "You for Sale: Mapping, and Sharing, the Consumer Genome,"*New York Times*, July 16, 2012, http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?pagewanted=all ("In essence, it's as if the ore of our data-driven lives were being mined, refined, and sold to the highest bidder, usually without our knowledge—by companies that most people rarely even know exist"); Natasha Singer, "Do Not Track? Advertisers Say 'Don't Tread on Us,'" *New York Times*, October 13, 2012, http://www.nytimes.com/2012/10/14/technology/do-not-track-movement-is-drawing-advertisers-fire.html ("But what is really at stake here is the future of the surveillance economy").

57. Julia Angwin, "The Web's New Gold Mine: Your Personal Secrets," *Wall Street Journal*, July 30, 2010, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

58. See Jim Harper, "Schneier on RealAge.com: Factually Incorrect," *Technology Liberation Front*, April 28, 2009, http://techliberation.com/2009/04/28/schneier-on-realage com-factually-incorrect/.

59. The European Union issued a directive in 2011 that requires explicit consent to place a cookie on a user's computer, but the directive has proven difficult to translate into enforceable regulation. See "Will UK.gov Crack Down on Itself for Missing Cookie Law Deadline?" *The Register*, May 18, 2012, http://www.theregister.co.uk/2012/05/18/most_gov_websites_will_miss_cookies_law_deadline/.

60. Marshall McLuhan, *Understanding Media: The Extensions of Man* (New York: McGraw-Hill, 1964).

61. The Privacy Act of 1974, Pub.L. 93-579 (1974). For recent interpretation, see *FAA v. Cooper*, 131 S.Ct. 3025 (2012). Cooper sued the government when Social Security Administration personnel revealed details of his health status to the Federal Aviation Administration, where he was licensed as a pilot.

62. Or worse, so general as to be serviceable by any ambitious agency or prosecutor eager to fit high creepy factor activities that were clearly not in the minds of those who voted for the legislation. A good example is the Computer Fraud and Abuse Act, 18 U.S.C. §1030, which prosecutors have tried—ultimately without success—to use in place of nonexistent laws against cyberbullying and employee appropriation of company data. See Larry Downes, "Lori Drew Verdict Finally Overturned," Stanford Center for Internet and Society, August 31, 2009, http://cyberlaw.stanford.edu/node/6246, and "US will not Challenge Computer Fraud Case to High Court, *NBC News.com*, August 9, 2012, http://www.technolog.msnbc.msn.com/technology/technolog/us-will-not-challenge-computer-fraud-case-high-court-932764.

63. Sheldon Richman, "Dissolving the Inkblot: Privacy as Property Right," *Cato Policy Report* 15, no. 1 (1993).

64. Lawrence Lessig, "Privacy as Property," *Social Research* 69, no. 1 (2002).

65. Ibid.

66. See Larry Downes, *The Laws of Disruption* (New York: Basic Books, 2009), chap. 2, "The Weird Economics of Information," pp. 25–44.

67. According to the Pew Internet and American Life Project, "Two-thirds of those who download music files or share files online say they don't care whether the files are copyrighted or not." Amanda Lenhart and Mary Madden, "Music Downloading, File-Sharing, and Copyright," Pew Internet and American Life, 2003, http://www.pewinternet.org/Reports/2003/Music-Downloading-Filesharing-and-Copyright/Data-Memo.aspx.

68. See Richard A. Posner, "Why There Are Too Many Patents in America," *The Atlantic*, July 12, 2012, http://www.theatlantic.com/business/archive/2012/07/why-there-are-too-many-patents-in-america/259725/.

69. R. H. Coase, "The Problem of Social Cost," *Journal of Law and Economics* 3, no.1 (1960).

70. R. H. Coase, "The Nature of the Firm," *Economica* 4, no. 16, (November 1937): 386–405.

71. See, for example, Jeff Gelles, "Verizon Wireless Policy Change Raises Privacy Issues," *Philadelphia Enquirer,* October 20, 2011, http://articles.philly.com/2011-10-20/business/30301830_1_verizon-and-verizon-wireless-privacy-policy-new-advertising-program.

72. *See* Cal. Civ. Code §3344 (1984); NY CLS Civ. R. § 50 (2000).

73. *Haynes v. Knopf*.

74. Nicholas Lemann, *The Promised Land: The Great Black Migration and How it Changed America* (New York: Vintage, 1991).

75. *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).

76. The case might have had a different outcome in the European Union, which is working out the specifics of a "right to be forgotten," which EU regulators see as a natural extension of the EU's more abstract privacy directives. See Larry Downes, "My Own Private Memory Hole," *CNET News.com*, November 16, 2010, http://news.cnet.com/8301-13578_3-20022977-38.html.

77. Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.

78. There are similar examples of laws regulating private sector use of information in health care, lending, mortgages, and laws that prohibit discrimination in housing, lending, insurance, and employment based on specific data such as age, race, ethnicity, gender, and other characteristics long associated with irrational prejudices. Which ones satisfy the criteria described above and which were necessitated by genuine market failures are questions well outside the scope of this essay.

79. Lessig in fact dodges even further. "The property right I am imagining governs the terms under which one machine can access certain data from the other machine. It says that the party who would collect these facts cannot do so without permission from [my computer]. The default is that the facts cannot be collected, but that default can be negotiated around." It is clear that by "certain data" he means "private" data, but the article never says so explicitly, nor answers the question of how that class of data would be defined.

80. Natasha Singer, "Consumer Data, but Not for Consumers."

81. For origins of the phrase, see R. Polk Wagner, "Information Wants to Be Free: Intellectual Property and the Mythologies of Control," *Columbia Law Review* 103, no. 4 (May 2003): 995–1034.

82. Marshall McLuhan, *Understanding Media: The Extensions of Man* (New York: McGraw-Hill, 1964).

83. See F. Gregory Lastowka and Dan Hunter, "Amateur-to-Amateur: The Rise of a New Creative Culture," Cato Policy Analysis no. 567, April 26, 2006 http://www.cato.org/publications/policy-analysis/amateuramateur-rise-new-creative-culture.

84. The RIAA has been pursuing its sole litigated case since 2008 against Jammie Thomas-Rasset, who was found to have shared 24 songs without authorization, leading to statutory damages of $1.5 million. The case has become a public relations nightmare for the industry. See Greg Sandoval, "RIAA Files Appeal in Jammie Thomas Case," *CNET News.com*, August 22, 2011, http://news.cnet.com/8301-31001_3-20095566-261/riaa-files-appeal-in-jammie-thomas-case/.

85. Sarah McBride and Ethan Smith, "Music Industry to Abandon Mass Suits," *Wall Street Journal*, December 19, 2008, http://online.wsj.com/article/SB122966038836021137.html.

86. Kevin Kelly, "Better than Owning," *The Technium*, January 21, 2009, http://www.kk.org/thetechnium/archives/2009/01/better_than_own.php.

87. Larry Downes, "The End of Software Ownership—and Why to Smile," *CNET News.com*, September 20, 2010, http://news.cnet.com/8301-1001_3-20016 864-92.html.

88. Kelly.

89. Ibid.

90. See generally "Big Data: The Next Frontier for Innovation, Competition, and Productivity," McKinsey Global Institute, 2011, http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation.

91. This is especially important for mobile apps, where screen real estate is limited and the ability to convey detailed information is constrained even further. See Tanzina Vega, "Industry Tries to Streamline Privacy Policies for Mobile Uses," *New York Times*, August 14, 2011.

RELATED PUBLICATIONS FROM THE CATO INSTITUTE

Reputation under Regulation: The Fair Credit Reporting Act at 40 and Lessons for the Internet Privacy Debate by Jim Harper, Cato Institute Policy Analysis no. 690 (December 8, 2011)

Electronic Employment Eligibility Verification: Franz Kafka's Solution to Illegal Immigration by Jim Harper, Cato Institute Policy Analysis no. 612 (March 6, 2008)

Amateur-to-Amateur: The Rise of a New Creative Culture by F. Gregory Lastowka and Dan Hunter, Cato Institute Policy Analysis no. 567 (April 26, 2006)

Understanding Privacy—and the Real Threats to It by Jim Harper, Cato Institute Policy Analysis no. 520 (August 4, 2004)

Human Bar Code: Monitoring Biometric Technologies in a Free Society by F. Gregory Lastowka and Dan Hunter, Cato Institute Policy Analysis no. 452 (September 17, 2002)

Internet Privacy and Self-Regulation: Lessons from the Porn Wars by Tom W. Bell, Cato Institute Briefing Paper no. 65 (August 9, 2001)

Capital Markets: The Rule of Law and Regulatory Reform by Solveig Singleton, Cato Institute White Paper (September 13, 1999)

RECENT STUDIES IN THE CATO INSTITUTE POLICY ANALYSIS SERIES

715. **Humanity Unbound: How Fossil Fuels Saved Humanity from Nature and Nature from Humanity** by Indur M. Goklany (December 20, 2012)

714. **On the Limits of Federal Supremacy: When States Relax (or Abandon) Marijuana Bans** by Robert A. Mikos (December 12, 2012)

713. **India and the United States: How Individuals and Corporations Have Driven Indo-U.S. Relations** by Swaminathan S. Anklesaria Aiyar (December 11, 2012)

712. **Stopping the Runaway Train: The Case for Privatizing Amtrak** by Randal O'Toole (November 13, 2012)

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress. Contact the Cato Institute for reprint permission. Additional copies of Policy Analysis are $6.00 each ($3.00 each for five or more). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Ave., N.W., Washington, D.C. 20001 or call toll free 1-800-767-1241 (8:30-4:30 eastern time). Fax (202) 842-3490 • www.cato.org