UNC SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 90
Number 5 *Social Networks and the Law*

Article 3

6-1-2012

Putting Consumers at the Heart of the Social Media Revolution: Toward a Personal Property Interest to Protection Privacy

Timothy D. Sparapani

PUTTING CONSUMERS AT THE HEART OF THE SOCIAL MEDIA REVOLUTION: TOWARD A PERSONAL PROPERTY INTEREST TO PROTECT PRIVACY*

REMARKS BY TIMOTHY D. SPARAPANI**

Thank you to the UNC Law Review, Professor Anne Klinefelter, Andrew Kasper and others for the invitation to speak. Commissioner Brill, distinguished professors and soon-to-be distinguished students it's a pleasure to be with you. These are my first public remarks since leaving Facebook.

My premise for my remarks is that despite what will shortly be one billion active Facebook accounts and several million social apps, the long-term viability of the social media revolution is not yet certain. I'm someone who wants to iron out the wrinkles by offering some proposals to help keep this revolution on track.

Disclaimer: Before I say another word let me be clear that my remarks today are solely my own. They are not those of Facebook, the ACLU, or anyone else. Any errors of logic or fact are mine and mine alone.

The value they may provide is solely of my making, but let's be honest, they are probably only worth as much as you have paid for them.

Let me apologize in advance to the full-time legal scholars in the room. I don't intend to provide a deep exegesis of current scholarship on privacy or social networking. I'll leave that to the law professors.

Let me also apologize to those scholars and experts in the room who have been especially influential to me and the development of my thinking. My attempts to synthesize disparate thoughts and strains of concepts are my own. The botched attempt to pull from them something useful and worthy of public utterance is again, solely my own.

** Former Public Policy Director, Facebook, Inc.; former Senior Legislative Counsel for Privacy Rights, ACLU.

Disclaimer #2: I maintain a reputational interest in Facebook's success. I am no apologist for Facebook. My former employer has made mistakes, some of which are clear and some of which will only be revealed in time. In the main, however, I think Facebook has gotten its policies and products correctly situated the lion's share of the time. And time and time again, where Facebook has erred it has quickly adjusted to respond and change course. That makes me a contrarian, I suspect. It also makes me a bit of a heretic in some privacy advocacy circles.

Disclaimer #3: I maintain a financial interest in Facebook. It's future economic success will redound to my benefit so discount everything I suggest as you will with that fact in mind.

Disclaimer #4: I fervently maintain that consumers are, in the main, rational, intelligent beings that are capable of making true choices for themselves with the information they are provided.

I oppose, reflexively, attempts by governments, advocacy organizations, or companies to dictate to consumers the amount of privacy that is appropriate for each individual.

I exempt, of course, certain traditionally protected classes—children, the elderly, the intellectually impaired, etc., whose ability to reason and make rational choices may be limited or diminished.

In the main, I believe that consumers are not only capable of making wise choices, they are in fact increasingly comfortable in making clear and granular choices about how much privacy they want and need.

I've observed how these choices change over time and vary by situation, geography, demographics, etc.

As a result, I've come to disfavor laws or regulations that mandate a set amount of privacy for individuals. For those of you who, like me, have tried to draft legislation before you may have experienced the feeling of being confounded by attempts to draw bright lines *for* consumers as opposed to attempting to draw statutes that employ bright lines that may be selected *by* consumers.

Disclaimer #5: I'm unabashedly, unapologetically, and unrelentingly pro-consumer in my framing. I start with the premise that the best outcome is not one that produces the most efficient result, or the result that produces the most net societal wealth. Neither, however, am I absolutely in favor of the result that maximizes the most total societal privacy.

Rather, I seek the outcome that favors each consumer in his or her individual capacity.

I take it as axiomatic that what we have known remains true and will increasingly be true in the future. Each consumer has an attitude that falls somewhere along a very wide spectrum of attitudes about how much privacy they want. Some will want maximal privacy to the point of preferring a hermit's existence. Some will want minimal privacy to the point of exhibitionism. Most of us will fall somewhere along the continuum in between.

And, make no mistake it is a true continuum. If my experience at Facebook proved anything, it is that with a data set of more than 800 million active users we needed to design a system that allowed users to choose at least 800 million different varieties of social networking privacy.

Disclaimer #6: I believe the FIPs, the Fair Information Practices, still have much value but they remain largely aspirational and unrealized.[1] Notice and choice can and still should guide corporate design in a way that treats consumers as intelligent, sentient beings, which I believe they are. But, we all—corporations in particular—have to strive to make them real and make them actionable. Part of this should be accomplished through the FTC and other regulators encouraging competition over these issues.

Disclaimer #7: Although my remarks today will focus on how the law of privacy can best be rethought to empower consumers in the era of social networking and social applications, I remain more concerned about governments than corporations. It is my contention—and here my ACLU background shines through—that the public has more to fear from government surveillance and the people with the guns and tanks and the ability to imprison people, than it does corporate amalgamations of data about citizens. Most frightening of all is the combination of corporate data gathering and parsing capacity with the authority and desire by certain regimes to disenfranchise, monitor, control, and thwart their citizens. Thus, my remarks today should be taken in the context that my bias is that while powerful corporations have great capacity, they are generally benign and usually, at worst, lousy, but not often inherently dangerous.

Final Disclaimer: I will try to leave time at the end of my remarks for us to engage in some Q&A. I must say at the outset, however, that due to the terms of my Non-Disclosure Agreement and its

1. *See Fair Information Practice Principles*, FTC, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited May 8, 2012).

confidentiality requirements there may be questions that you ask that I cannot answer.

You may feel free to disagree with any of my premises and disclaimers, but at least I've tried to humbly unearth them for you at the outset.

Now that I've lowered expectations sufficiently, let me briefly summarize what it is I hope to accomplish in my remarks today.

I am here to argue that the social networking revolution's prospects will be diminished if consumers are not placed at the center of the revolution by social media companies and governments. To do that I recommend the enactment of a privacy statute that treats privacy as an individual property interest. I also recommend efforts by the FTC to further this property interest. I will try to make ten interrelated points:

1. Internet Companies—Including Social Networks—Must Increasingly Deliver Real Value to Consumers, but Most have the Balance Backwards

Most startups use consumers instead of being used by consumers. That is a dangerous reversal of the value equation and leads to righteously angry consumers, regulators, and Congress members. Social networks and apps built on top of them, must continue to innovate in terms of the value they produce for consumers, not just in terms of their ability, to ever more successfully monetize consumer data.

2. Rebalance the Section 5 Unfairness Test[2]

The FTC should use its unfairness powers to evaluate social media companies, rather than leaning almost entirely on its deception prevention authority, as it has to date. In doing so, the FTC must be mindful to encourage companies to innovate, and the FTC can do so by examining the "countervailing [public] benefits" these companies provide when determining whether a corporation has acted unfairly. I see little evidence that a key statutory phrase built into the "unfairness" statute as a balancing test is being given regulatory meaning. I do not mean to say the FTC's authority should be stripped or limited. Quite the opposite. Rather, I think that if the FTC evaluates social media companies in light of their "countervailing

2. Section 5 of the Federal Trade Commission Act provides: "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices affecting commerce, are hereby declared unlawful." 15 U.S.C. § 45(a)(1) (2006).

[public] benefit" they will prod social media companies to produce more products for consumers rather than increasingly using consumer data as the product. A survey of recent FTC enforcement actions does not find language suggesting this balancing test is occurring. Of course it may be happening behind the scenes when the FTC determines whether to pursue a particular matter, but this is like that old adage about grading in math class. If you don't show your work, you don't get credit for the effort. My experience from inside a company suggests that companies are carefully watching every step by the FTC and that they would respond to a regulatory signal. In the absence of this sort of signal, companies are less likely to innovate for fear of running afoul of the FTC. Over time, that can rob social media of some of its vibrancy. Giving more prominent attention to this public benefits test may empower consumers by modifying corporate behavior. This language is not mere legislative surplusage and should not be treated as such.

3. Quasi-Property Privacy Theory

In the social media age we need a quasi-property theory of privacy to replace our current hybridized and inconsistent quasi-tort-based, quasi-rights-based model for protecting privacy. To sufficiently advantage consumers and protect them, I argue that we should engraft upon these a quasi-property system that empowers consumers to make rational choices on their behalf. Quite by accident I reached some of the same conclusions that Boalt Hall Professor Paul Schwartz did in advocating a property theory of privacy as a better guarantor of personal privacy. Schwartz argued for this approach in a 2005 *Harvard Law Review* article entitled *Property, Privacy, and Personal Data.*[3] He advocated for what he termed a "use-transfer restriction" regarding personal data, and I endorse that limitation.

4. Most Privacy Injuries Anticipated from Social Networking Are Not Caused by Social Networks but by Third Parties Misusing Information Acquired from Social Networks

Facebook, LinkedIn, Twitter, Formspring, etc., may be the handmaiden of broader distribution of sensitive information, but often that distribution is intentional by consumers. Even more often, it can be fairly said that the sharing of information with a social network for certain purposes is authorized and deliberate. Consumers often use the social network as an intermediary to obtain goods,

3. 117 HARV. L. REV. 2055 (2004).

services, and entertainment at low or no cost. To this end, enforcement should be retargeted to deter third parties who are not explicitly authorized by consumers from accessing and using consumers' information.

5. Empower Consumers To Capture Full Benefits of Social Networking

The proactive legislative model I propose be enacted into statute would give consumers the right and opportunity to authorize sharing with certain third parties for certain purposes via a social networking pass through or platform. It would empower consumers, however, to also forbid the sharing of info with third parties in situations where we can anticipate real, cognizable injury.

6. Enforcement of Privacy Rights in This Proposed Regime Can Be Better Targeted; Responsible Companies Can Be Separated from Irresponsible Companies, and Consumer-Facing Companies Can Be Separated from Non-Consumer Facing Companies with Respect to Statutory Requirements and Enforcement Actions

The Do Not Call statute,[4] arguably the most successful privacy statute of the last 50 years, points the way forward. Companies with an "Established Business Relationship" are—and should be—granted more opportunities and leeway for their interactions with consumers under that statute. We ought to emulate that in future privacy statutes. Doing so gives meaning to the Fair Information Practice of Notice and Choice.

7. The FTC, States Attorneys General, and Data Privacy Commissioners Around the World Should Refocus Their Energies on Preventing Cognizable Harms That More Closely Mirror a Property Injury

The focus on reputational harm, in other words, giving more credence to the tort-style view of privacy, is inherently weak and does not fully protect consumers. Enforcement is always post hoc and often unsatisfying to consumers. I am not arguing that we should scrap this effort but rather that we emphasize other harm mitigation in our enforcement efforts. Similarly, I think we are heading toward the end of the period of time when enforcement actions that are

4. Do-Not-Call Implementation Act of 2003, Pub. L. No. 108-10, 117 Stat. 557 (codified at 15 U.S.C. §§ 6101–6155 (2006)).

based on privacy policies or a lack of basic security for sites will substantially improve outcomes for consumers.

8. Corporate Free Speech Cannot Trump All Privacy Rights

Let me argue against unlimited rights for a minute. The United States Supreme Court's decision in *Sorrell v. IMS Health*[5] probably needs to be revisited and or limited. Allowing corporations to effectively "own" and use in an unlimited way consumers' information is an exception that, if left unaddressed, extinguishes each consumer's potential privacy property right. Further, an unlimited speech right for corporations grounded in the ability to use consumer data could be—and likely will be—taken to absurd lengths and will disempower some consumers who would otherwise protect their privacy.

9. Although I Argue that Corporate Free Speech Rights in Data Cannot Be Unlimited, Whatever Regulatory System Societies Ultimately Adopt Must Preserve the Ability of Companies To Innovate, Including the Ability To Provide New Goods, Services, Efficiencies and Compete on Privacy Protections

The path forward to increase the total quantum of consumer benefit is a regulatory model that encourages companies to innovate and grow. That means we must all accept some experimentation with the use of consumer data so that social networks and social apps can provide valuable new tools for consumers. Similarly, the regulatory scheme should embrace innovation to ensure a commensurate improvement in privacy protection by companies with respect to products and policies.

10. Finally, the Social Revolution Is Likely To Rise or Fall Depending Upon Whether We Enact Consumer Empowering Systems Similar to Those I've Suggested

So it is a minor thing. That's all I'm predicting. Not exactly fire and brimstone, hellfire and damnation, but pretty darned close if you live in Silicon Valley. In short, consumers likely will, at best, curb their use of and engagement with social networks and social apps unless they are put at the center of the social revolution and the laws that will guide it. At worst, some segment of consumers, those that

5. 131 S. Ct. 2653 (2011) (finding a state statute that barred the sale of pharmacy records that revealed the prescription practices of physicians in violation of the First Amendment's free speech protection).

want the most privacy or who do not clearly experience substantial benefits, may stop using social networks or social apps altogether. If that occurs, then the total benefit to the remaining individuals using social networks or social apps will be diminished, as will be the overall benefit to society from those social tools. It is a truism but worth articulating; that is because every person who does not use a social tool makes that tool less social.

Now after that not-so-short summary, here is a deeper explanation of my proposed regime. Here's my first observation: Internet Companies—including social networks—must increasingly deliver real value to consumers, but most have the balance backwards.

Right now, social networks are positioned as producing benefits for the individual members. They are a place to commune with friends, colleagues, etc. To learn and share the experiences of your life and of those whom you are acquainted with. Same with Internet sites. The model is the same. The website offers you a good or a service and an efficiency to reduce the amount of work of doing the same thing in the offline world. But of course there's a catch. Businesses operate as businesses and do not provide these services out of the sheer goodness of their heart. Consumers aren't dummies and of course they understand that. Given all the attention the tradeoffs have received, we can assume as privacy practitioners that most consumers understand in a general way that there are real tradeoffs involved with sharing their data with companies. Most consumers, however, are willing to accept those limited tradeoffs of sharing data with particular companies whose brands and services they know and want for the purpose of obtaining the benefit that is at the heart of the website or social network.

That seems like a fair and healthy balance for me with the currency being consumer data exchanged knowingly and willfully by consumers for the provision of a clear product, service, or benefit. In many cases, we can postulate that consumers come out ahead in that deal, particularly when we are talking about a "free" web-based service.

But, the balance of the equation has and will continue to shift as the most sophisticated minds in Silicon Valley design ever more clever ways to utilize disparate data about us—data that until relatively recently was little more than incidental meta data—to profit from us without providing consumers additional commensurate value. I'm referring here to location, proximity of friends, time and date stamp of log-ins, logging frequency, mobile usage, network of friends,

etc.—data fields that until recently had only theoretical value. In this emerging world of innovation it can be increasingly said, as some have already observed, that "if you don't know what the product is of a website or social network, then *you* are the product."

If I learned anything at Facebook I learned the centrality of a corporation maintaining consumer trust as a central business proposition. When services are free on the Internet and the barriers to entry for competitors are relatively low, the loss of consumer confidence in a corporation can severely damage or even doom a corporation. As cavalier as Facebook might have seemed to all of you here who are especially sensitive privacy practitioners, and as often as the news reported disparagingly about the choices Facebook made regarding consumer data, I can report to you absolutely that there was an ongoing, running battle of wills within Facebook about how to preserve consumer trust. Battle-scarred Facebook veterans preached this to the newbies. Disagree as you will—and I often did—with the final decisions on products and policies emanating from Facebook, but the internal debate almost always considered the impact on user trust. Sometimes Facebook got it right despite public outcry and, other times Facebook quickly adjusted to respond to consumer sentiment.

The risks to upstart social networks, social apps, or other new web services are perhaps even greater since the startups will lack the mass of users that provide business value to these entities' advertisers. Social startups are also at risk to lose consumers over privacy and related trust issues because until they have been adopted by consumers en masse and those consumers have adopted use of the startup as a lifestyle or habit, they also lack the "lock in" that keeps consumers using the same product or service despite potentially better competitors' options out of force of habit and due to familiarity. I'm disparaging neither, but the most obvious examples of lock in being a real force are the extraordinary current user bases of AOL and Yahoo!. Despite being relatively ancient companies founded well before the social media revolution, both still have enormous and loyal customer bases.

It's my supposition that as consumers increasingly understand that metadata about them is being monetized by established companies offering new services and/or new startups with brand new offerings, consumers will ultimately demand new value be delivered to them that is roughly commensurate with the data they are inadvertently disgorging. For consumers to continue to use social

apps and social networks, companies will have to couple their increasing use of data with real value.

Certain trends in technology are observable and need to be accounted for in this data-for-value equation. The trends are largely synergistic in that the combination of the trends both facilitates new technological possibilities and raises potential new privacy concerns.

Most of this is well known, but let's review briefly. Here's what we know:

1) The devices we use are ever more powerful, and more power means that devices can do more things simultaneously. This will increase the tendency toward convergence so that the phones we've used to get us on the Internet, play music, and function as TVs, will also now serve as identity verifiers, and process payments in a cashless manner. This means that the devices will produce more metadata. Lots and lots more metadata.

2) The world has gone mobile. Our devices provide very precise and personally identified signals to companies about where we are, whom we are with, where we've been, and what we have just purchased. This allows companies to predict with increasing sophistication where we are going, where we will spend our money, what we'll want, need, and buy, and whom we will do it with.

Put that all together, and social companies are salivating. Companies pushing our friends' recommendations to us will mean we are increasingly guided toward making certain decisions about our purchasing—and it'll happen in darn near real time based on our exact location and likely based on whom we are with at that time.

The value proposition for consumers is there but needs to be kept foremost. Will we get real-time digital coupons or will only certain "preferred" consumers be favored in terms of pricing for goods, services, and value. Will our typical location cause us to be redlined out of opportunities or will some be disproportionately advantaged due to the neighborhoods they live and work in while the rest of us serve as consumers that subsidize those lucky one-percenters' purchases?

Ultimately, I am arguing that in order for "social" functions to have broad market appeal and adoption by broad swaths of consumers, companies will have to increasingly turn our location into advantages for all of *us*, rather than as a means of *distinguishing amongst us* as consumers in ways that would make many of us uncomfortable at best. It's a fundamental question to be answered; Will the metadata we cast off in our daily lives be used to discriminate

against us as consumers or provide us with efficient access to goods and services? Put another way the question is this: Will data empower us or will it be simply used to more efficiently commoditize us?

So my second point is that *the Federal Trade Commission could do more to encourage social networks* and Web 2.0 sites to add consumer value by giving real force and effect to seemingly long-ignored language in their section 5 authority. It is section 5 of the FTC Act that gives the FTC authority to take action against companies that are engaging in "unfair or deceptive" trade practices. But the clear language of section 5 requires the Commission to engage in a balancing test. Part of that test is to review the practice being considered in light of any "countervailing [public] benefits" that the practice provides. I've done a fair amount of review, but not an exhaustive review, of cases and haven't seen language from decisions that suggest the FTC is engaging in a real assessment of consumer benefit in the Internet concept. It could be that this is because most of the Internet age decisions are primarily "deception" cases, not "unfairness" cases, but the point stands. This statutory language is not mere surplusage. Congress intentionally chose to make this part of the unfairness analysis.

My supposition is this: If the FTC were to more explicitly dangle this carrot in front of cutting edge Web 2.0 companies, some of those companies might be more willing to expend additional energy to produce additional and obvious consumer benefits while they were deriving innovative uses for consumer data for the corporation's benefit.

There are additional ways to encourage consumer value. My third point—in order to protect against the downside of the aforementioned technology trends—is that *we need to move to a quasi-privacy theory of property*. By that, I'm suggesting that if *we* are increasingly the product of the social networking revolution, then we all as consumers ought to have some ownership over the data in a manner that lets us think and act like consumers. Because our data has a value we ought to be able to help consumers capitalize on it, not just be injured by its misuse and then try to receive post-hoc recompense for privacy injury through tort claims that may provide some recompense for reputational harm but are unlikely to deter true misuse of personally identifiable information. If we think of our data as a property interest, it allows models to develop that allow consumers to be free to rationally share their data in a limited way to receive a benefit from a company in return. If I trade my data knowingly and intentionally for a benefit for a set period of time or

only to receive a certain type of benefit, but do not trade all of my ownership of that data in perpetuity, my bargaining power as a consumer increases substantially.

Companies have acted as if when a consumer gives them personally identifiable data the company can keep that and use it in perpetuity and do whatever they want including selling it to other third parties. But of course that's not what consumers intend. If the law recognizes a property interest, then consumers can more carefully limit sharing they would never have intended.

Thankfully, smarter people than I have reached the same conclusion. Quite by accident I reached the same basic conclusion that Berkeley's Paul Schwartz did in 2005. He was building on and in part responding to concepts pushed by Larry Lessig. I'm aware of Marc Rotenberg's forceful refutation of this commodification theory. But let me say that I'm a realist in that like it or not, society has allowed the development of personally identifiable information as a commodity. I share Marc's feeling that this is deplorable, but I am searching for a response to the world as it is, not as I would ideally like it to be.

Fourth point: Although Facebook captures all the attention and anger of consumers, the press, legislators, regulators, and law professors, *many of the concerns that have been raised about privacy risks from social networking are only realized when third parties other than the social networks or social media use data against consumers.*

Of course, Facebook and other social networks play an essential role in compiling and making public more of that data, or in pushing the data out in new ways that consumers didn't expect, or in failing to safeguard it from being shared with or scraped by third parties. Surprises created by shifting privacy policies or changes that expose previously hidden data are part of the problem. All social networks, and other internet-based, consumer-facing companies have a responsibility to prevent data sharing consumers never intended. Where they fail regulators should act.

It seems to me, however, that where the real injuries can occur is when unknown or unexpected third parties obtain data through purchase or scraping and then use it to make decisions about people that have a quantifiable economic impact. I worry deeply about reports that insurance companies are trolling social networking sites to find info to help them deny claims or to redline people from certain demographic blocks out of coverage altogether. I am troubled by data brokers scraping social networks and selling data to any business that will buy it as this could lead to the same sort of

discriminatory pricing scenarios I just mentioned. I'm troubled by universities and colleges previewing applications for admission online and finding information that they will use to make judgments about the worthiness of their applicants. And, I'm especially concerned about employers using social networking information never intended for their eyes to make hiring and firing decisions.

This leads to my fifth point. To further ensure that consumers are protected and that the social revolution is a successful one, we should consider an entirely new direction in privacy legislation from the one Congress has been taking. Instead of a Do Not Track privacy bill, we need a Do Not Sell bill that prohibits Web 2.0 companies from selling consumer data to random third-party companies with no relationship to the consumer whose data it is. That should be paired up with legislative prohibitions that limit third parties' use of consumer data that they do not have authorization from the consumer to use. Thus, I propose that we also need a Do Not Redline, Do Not Price Discriminate, and Do Not Use set of legal limitations that would keep insurers, merchants, colleges, universities, and employers from using data that is not public to deny individuals an educational or economic opportunity. The goal is to make that quasi-property interest real for consumers by giving them the ability to choose to share with a third party through a social network. If the consumer believes they can get a benefit from doing so, then they may. Thus, if a consumer wants a social network to share their data with other businesses to get the consumer discounted pricing, or accelerated matriculation, or a speedier background check, they could authorize that. However, if they don't, they'd be able to limit the sharing by Web 2.0 companies as of right.

There's clear precedent for this approach, which is my sixth point. *I'm arguing there is something meaningful in privacy rights about distinguishing in law between a first party and third party.* The first-party company that a consumer intentionally interacts with online ought to have more leeway with consumer data than does a third party. I think that's especially true where the first party does not transfer the data to the third party unless a consumer authorizes that data sharing. I think it is even more true when that company is a public-facing company, e.g., a brand or entity the consumer knows is a recipient and user of their data as opposed to a company whose presence is either obscured or entirely invisible to the online consumer. Thus, a wise quasi-property privacy regime would track the FIPs carefully and give notice and choice real meaning in online interactions. If a consumer has notice about which company in

particular they are interacting with online they can arguably make a clear, meaningful choice whether to share data with that first-party company.

The Do Not Call statute, arguably the most successful privacy legislation of recent vintage, doesn't just flatly prohibit the annoying corporate calls to people who don't want them. Instead, it has an exception from the call prohibition for those companies that consumers already have an "Existing Business Relationship" with. Consumers establish those Existing Business Relationships with a company by having previously conducted business with that company. Therefore, the privacy prohibition tracks directly with a consumer's preferences and choices. Those companies with this Existing Business Relationship have more opportunities with their customers based on the consumer having clear notice and choice about whom they are contacted by. We should recreate that notion in any new privacy statute. In fact, U.S. Senator John Kerry's legislation, S. 799, the Commercial Privacy Bill of Rights Act,[6] wisely incorporated this notion.

My seventh point is that the FTC, state Attorneys General, and the Data Privacy Commissioners around the world could make truly meaningful advancements in privacy protection of consumers by focusing on this first-party, third-party distinction. There ought to be concerted regulatory efforts brought to bear to limit or impede the data broker industry, which has a business model entirely premised on surreptitiously obtaining information about consumers as a third party, without consumer consent and then reselling that information to other third parties. This data broker industry thwarts meaningful consumer notice and choice, and it facilitates the very "property" or true economic harms I've identified. Services that crawl the web to repackage information and resell it allow companies to—in my opinion—inappropriately make decisions about whether to insure a person, or their credit worthiness, or whether they should be admitted to a university or college. If regulators focus on this black market in personal data that has escaped the boundaries of the intentional sharing of the individual whom the data is about, regulators could significantly diminish the potential downsides of the social networking revolution. That in turn would increase the chances that the benefits would greatly outweigh the burdens of this technological revolution.

6. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong.

My eighth point is that the Supreme Court got this badly wrong, in my opinion in last summer's decision in *Sorrell v. IMS Health.*

Simplified greatly, the Supreme Court decided 6 to 3 that a company's commercial free speech rights trumped the ability of the States of Vermont and New Hampshire to absolutely prohibit the sale of consumer data from a first-party company to third-party companies. In short, the Supreme Court seems to have given the green light to a black market in data sales and data scraping that ultimately thwarts the ability of consumers to have meaningful choice over the entities that can use data about them. I don't want to be too hyperbolic but it's as if the consumers' privacy rights were lifted entirely out of the equation.

The Supreme Court did leave some wiggle room in suggesting that if the statute at issue had allowed for resale of data under even a few narrowly tailored exceptions the law might have withstood scrutiny. That nod by the Court suggests to me a way forward out of this mess. If we had a property rights view of privacy, and if the law recognized a consumer's right to permit purchases of consumers' data from a first-party company, then we might have a solution to a variety of problems.

That exception to *Sorrell* would then allow social networks or social apps to be places online where consumers willfully and intentionally share their data.

Rules could be constructed, as I've previously suggested, that would allow for that data to be transferred to certain third parties—including data brokers—that the consumer intends to be able to obtain that data. Consumers could reasonably be expected to only permit that data transfer where there is a clear benefit they expect to obtain from that first-party social app transfer to a third party. That gives them meaningful control. It also gives them clear benefit. More importantly, it gives life to this quasi-property privacy theory I've concocted but allows the consumer to take off the table transfers to third parties that might use the data to do the consumer harm in his or her economic transactions, or diminish his or her educational or employment opportunities.

Without such an exception controlling the impact of *Sorrell*, the holding of that Supreme Court decision seems to give absurd amounts of unlimited access to consumers' private data to corporations. In that sense, the terrifying result of *Sorrell* allows the corporate First Amendment commercial speech right to swallow whole the individual consumer's right to privacy, or what I've termed their property interest in maintaining their privacy. That would be an absurd and

dangerous outcome because it means that it is open season on consumer's private data and that social networks and social apps can be turned into little more than game preserves for data brokers to go hunting for consumers' data.

Ninth point: Whatever legislative, regulatory, or judicial rules we concoct to limit *Sorrell* will create the best public policy and maximize the personal privacy of consumers most efficiently if they *tacitly endorse social networks and social apps' innovation.* Having worked inside a company that was innovating at astonishing speed, I witnessed first hand the ability of engineers to develop elegant solutions to vexing privacy, safety, and security problems. I marveled at the ability of coders to create solutions that were simultaneously pro-consumer and pro-social network because the consumers and the network's interests were aligned in preventing unauthorized third parties from obtaining access to consumers' data. We need to be sure that our attempts to limit the downsides of the social revolution do not hamstring these engineers but instead encourage them to compete on privacy, safety, and security grounds. A policy scheme that rewards companies for resolving the problem of unauthorized third-party data access can work in concert with the refocused regulatory efforts I've previously suggested to give real meaning and value to this quasi-privacy property theory.

My final point is that success or failure of the social media revolution may be dictated by whether society gets this right. Our failure to get this right will be profound. If we fail to put consumers at the center of the social revolution and the laws that will guide it, consumers likely will at best curb their use of and engagement with social networks and social apps. At worst, some segment of consumers, those that want the most privacy or who do not clearly experience substantial benefits may stop using social networks or social apps altogether. If that occurs, then the total benefit to the remaining individuals using social networks or social apps will be diminished, as will be the overall benefit to society from those social tools. It is a truism but worth articulating; that is because every person who does not use a social tool makes that tool less universally useful or, said in the Silicon Valley way, less "social" and, therefore, less valuable.

More importantly, failure means that social networks will be turned into the handmaiden of an unlimited and supercharged black market in personally identifiable information. This will be ultimately disempowering to consumers and bring about the very privacy risks we all worry most about.

In summary, I've called upon each segment of this social networking revolution to play a role in helping achieve the future success of this Web 2.0 world. Consumers can and must make intelligent choices as to which corporations they share their data with. Social networks bear a special burden to build the tools that facilitate true personal control over data and must work to eliminate unauthorized third-party access to data. Social networks and social apps must provide ever-increasing amounts of social value and utility that consumers, not other corporations, benefit from. Privacy laws must be enacted that explicitly put the consumer in control of whom they share with, what they share, and when. We have to give real meaning to that quasi-property privacy right I've tried to articulate. The FTC and other privacy regulators must refocus on preventing the types of true property harms—economic, educational, employment, etc.—that are likely to result from a failure to rethink their enforcement schemes. And, we've got to find a way to prevent the decision in *Sorrell*—from swallowing the social revolution whole through its green lighting of data brokers under the guise of protecting commercial free speech.

Thank you for your patience and attention.