Myths in the Privacy Debate

Duncan A. MacDonald

INTRODUCTION

I want to dispel some of the myths in the privacy debate, but I am not sure where to begin, because privacy is so hard to pin down. Like a myth itself, privacy can have a myriad of different meanings to different people at different times, and it has always been that way, even from antiquity.[1]

The desire for privacy probably originated as a survival instinct, the kind that drives animals to mark off and make claim to a special territory in which to hunt, live, procreate, and protect family from the reach of predators and competitors. As such, it is possessive and in a sense anti-others. In organized societies, it has a political texture that essentially is anti-authority. In its modern flowering, privacy is closely tied to property rights—private property as envisioned in Lockean political philosophy.[2] Not surprisingly, it thrives most abundantly in capitalist economies, especially those with strong traditions of upholding individual freedoms, like free speech and expression.

By and large, it is a dead letter in command economies, theocracies, and to some extent in homogeneous cultures.[3] People assert it in some places to undermine religious domination and in others to uphold religious and philosophical freedoms. As a rule of thumb, the bigger the governmental bureaucracy in any country, the greater likelihood that it will invade the privacy of its citizens and influence its social culture to cause citizens to do the same against each other.

Throughout history, privacy as a concept is seen always in transition, always being redefined by new information.[4] Contrary to current popular belief, technology more often than not has expanded its possibilities, mostly because of improvements in printing, housing, and transportation and distribution systems. The same holds true for economies with a growing middle class. As individuals accumulate wealth, their ability to weave private spaces into their lives increases.[5]

The intensity of the privacy debate today versus the debate in the past results from numerous factors. Certainly, the horrors of Nazism, fascism, and communism jolted Western nations into realizing how important privacy is and how easily it is lost. Most recently, the European Directive on Data Protection has challenged us to consider whether Congress should pass a similar data-protection law. The directive itself reflects the fear of the democracies of the European Union that information technology might be used in the future to subjugate people to private-sector dictators.[6]

Put another way, their fear is that technology will enable businesses to know enough personal information about people to manipulate their economic decisions. It is a fear that mysteriously disregards the possibility that people will learn to use technology to the opposite effect—for protection against economic control.

There is no question that businesses are using new technologies more than ever to collect information about consumers, but to a large extent the debate is about why they are collecting so much. Privacy advocates say it is to exploit consumers. But businesses say it is only to better understand what consumers want, so that they can supply it efficiently. They add that because today's consumers are more financially complex than they were a generation ago, they have no choice but to pursue whatever useful information they can find.

Without question, consumers own more, move around more, and buy more products from significantly more entrepreneurs than their forebears. And they pay with an ever-expanding variety of payment vehicles. A generation ago, they made most of their purchases as captives of local stores who knew them more intimately than any modern company could ever hope for. In contrast, today's consumers can transact anonymously on and offline with a seeming infinity of institutions across the planet, and thereby scatter their commercial information in ways that frustrate anyone bent on trying to figure them out.

But that is exactly what businesses must do to succeed. The laws of supply-and-demand require businesses constantly to

learn as much as they can about what consumers want. And the more particular and shifting consumers' wants, the deeper businesses must probe. This information-seeking process, of course, works both ways, with consumers having constantly to keep up with businesses and the vast array of their products and services.

THE MYTH THAT WE NEED MORE PRIVACY LAWS

Although businesses and consumers need free access to information about each other to serve their respective needs, our public debate is only about how the former collects and uses information. This paper will focus on myths in that debate, starting with two that attract the most attention, each a flip-side of the same coin. One is that US law is deficient on privacy; the other is that we need more laws to protect it.

On the contrary, there is an abundance of state and federal law in the US governing privacy in the public and private sectors—statutes, regulations, common law, and contractual rights—and it is growing rapidly.[7] At the top is the US Constitution, arguably the oldest and most successful privacy law in the world. The Constitution says a lot about privacy without ever mentioning the word. It doesn't have to, of course, because of its broad guarantees of fundamental freedoms and its strict limits on government actions that interfere in people's lives. The Constitution says, in so many words, that what people do with their freedom is their private business, not government's.

Thirty-five years ago the Supreme Court reiterated this principle in the much-disputed landmark decision of Justice William O. Douglas in *Griswold v. Connecticut*.[8] Perhaps more than any other Supreme Court decision in our history, *Griswold* opened a searing debate in America about privacy.[9] I want to argue that *Griswold* means government must stay out of private-sector privacy matters—and that means no regulation of business information practices, except in response to extreme situations, for example, to prevent crime[10] and abuse of sensitive personal information, like medical records. Whether it allows room to require disclosure of business information practices is open to question.

Griswold involved the punishment of an organization and its "Medical Director," who were in the birth-control business and whose crime was to prescribe contraceptives in violation of Connecticut state law. In upholding the decision of the Connecticut Supreme Court that the law in question violated "the right of marital privacy," Justice Douglas wrote, "[T]he First Amendment has a penumbra where privacy is protected from governmental intrusion." He called it a "peripheral right," and noted that "guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance." His closing words were that our "right of privacy [is] older than the Bill of Rights."

We should take *Griswold* on its face[11] and recognize that the First Amendment is the cornerstone of privacy in America; moreover, that its language protecting free speech, press, expression, religion, and assembly allows people to create sanctuaries—spheres of privacy—that enable a truly private life, without which, as *Griswold* says, the "express guarantees [could not be] fully meaningful." The First Amendment liberates people to think, write, and speak freely, hold alien philosophies, go where they want, be alone or in organized groups, practice traditional or new religions, reject religion altogether, withdraw from public life, transact regularly in commercial markets, and on and on. These rights are private, and that means government has no role to play in whether and how people choose to use them. It means government cannot occasionally deny or censor them, or interfere with peoples' beliefs or choice of friends, neighbors, or social/political organizations. It can intervene only in extreme cases.[12]

Griswold in effect tells us that privacy must be held to the same First Amendment standard as for free speech, press, religion, and assembly: When it comes to protecting those rights, citizens must fend for themselves. As with free speech, they must determine on their own what privacy means, and how and when to use it. And as with other First Amendment rights, they must learn how to pursue, protect, and exercise it through self-reliance.[13] As the opening words of the First Amendment state, government has no role here: "*Congress shall make no law.*"[14]

THE EXTINCTION OF PRIVACY?

To get around this injunction, privacy advocates rely on another myth—that privacy is at risk of extinction in America, due in good part to the Internet.[15] We are told, for example, that people use the Internet less than they would because of fear of losing their privacy. This is an exaggeration. Peoples' use of the Internet is increasing exponentially, perhaps more rapidly than for any other product or medium in history.[16] In 1999, Americans sent well-over one trillion e-mails, most of them unprotected by encryption. They accommodate the slight risk that others might spy on their e-mails because of their long usage of phones, which they know from experience are less protective, not to mention less versatile and more expensive.

Further belying a fear of the Internet, consumers' e-commerce transactions are growing at an explosive rate of 300 to 400 percent annually, notwithstanding the well-known fact that many Internet entrepreneurs capture and use consumers' browsing and transaction information for marketing purposes. Most consumers put up with this because they know they can: 1) get a better deal online; 2) block the information capture in most cases; and 3) resist any subsequent marketing solicitations that ensue. Under the *Griswold* view of privacy, they have little choice but to fend for themselves.

The First Amendment often puts consumers in this position. For example, when they shop on or offline for a movie, book, music CD, live entertainment, or just a TV or radio program, they will often encounter things that deeply offend their moral, political, religious, or civic beliefs. It might be sexually explicit advertising or songs that glorify sexism or violence. But whatever the case, the First Amendment will not allow them to turn to government for a remedy. It tells them, in effect, that their only recourse is to turn away. Or, if they are sufficiently motivated, to use their right of free speech to try to persuade the offenders to change their ways or to persuade others not to give them business. In either case, change can only occur through *private action.*

Private action has stood us well in the marketplace. The alleged risks that the Internet and information-technology

industries provoke are not unlike what other industries have faced and resolved without government intervention. Take any industry and look at its products ten, twenty, fifty, one hundred years ago. To pick an example, automobiles at the turn of the century didn't have a roof, doors, heating, front windows, a radio, air conditioning, or reliable tires—most of the conveniences we consider essential today. They broke down constantly and were very dangerous. But as the century rolled on, the auto industry, listening to consumers, effectively addressed these problems and got us to where we are today: reliable products that Americans love. But imagine if Teddy Roosevelt's Congress, at the dawn of automobiles, had the hubris to require the industry to fix the flaws in its cars immediately. Would we have better cars today?

Will we have a better information industry and wiser use of information technology in the future if government attempts to fix the perceived and anticipated privacy flaws of both, instead of leaving the quest for solutions to free markets? Will regulation lead to efficient, cost-effective privacy protection? Since free markets have given us so many of the privacy opportunities we have today, and since government historically has been the greatest threat to privacy, why would anyone prefer the latter?

The point is simple: Economic markets create competitors and put them through an unending, rigorous process to win consumer favor through invention, product improvement, attractive packaging, efficient distribution, customer service, price, trust, and scores of other attributes. Markets respond to flaws in every industry, figure things out, and provide value without government involvement. There is no reason, therefore, to believe that the burgeoning information industry, which has so richly enhanced our lives, will nonetheless uniquely fail us on privacy protection.

In many respects, the information industry represents a triumph of the First Amendment—the maximum, historically-unparalleled democratic flow of information to ensure individual autonomy. It is only natural that there is some confusion about how best to deal with the mass of information it makes available to everyone. But it is foolish to suggest at this early stage of the

industry that government should intervene to set things right. Trial-and-error in the market and consumer self-reliance will do that, as they always have.

Privacy advocates, therefore, should pay close heed to *Griswold* and the First Amendment's admonition that *"Congress shall make no law"* governing privacy—no government intervention, except in response to extreme situations. Short of an extreme, the Constitution trusts private forces will work things out.[17] Accordingly, there should be no privacy legislation if: 1) the privacy harm is not definable, serious, and provable (*i.e.* is based only on a guess about what might happen); 2) the harm is of a kind that the marketplace has effectively resolved in the past without government intervention; 3) consumers can deal with the harm on their own without significant cost and effort; 4) the harm shows signs that it will abate through industry self-regulation, new protection technologies, or consumer education, self-reliance, or acceptance of *quid pro quo* (*i.e.* value for what is given up); 5) it discriminates by applying only to business practices and not to all other organizations that engage in similar practices, such as government agencies, schools, charities, political parties, *etc.*; 6) the legislation will cost consumers more than the harm it seeks to eliminate; and 7) there is another constitutionally-less-harmful alternative. To be safe, the new legislation should have a quick sunset, because privacy considerations change rapidly and privacy risks are constantly reduced by new inventions and business practices.

Based on what we know about the status of privacy in America today, it would seem that few, if any, new laws are justified. Privacy is not seriously being harmed by industry, and, in any event, consumers have the means to manage what they don't like. They can utilize a number of tools to protect themselves in the face of a perceived privacy risk—or they can accept the risk in return for an economic benefit.

THE MYTH OF MANIPULATION

The privacy cognoscenti won't buy this. They are riled not only that businesses compile and mine information they get

on and offline; they are also convinced that businesses use the information to manipulate consumers. Most importantly, they believe the manipulation will be successful. They have to believe this, for without the certainty of manipulation their case that privacy harm is serious falls apart. What is left for them to hang their hats on? Junk mail, occasional telemarketing calls, information that slumbers in a database until it goes stale, customized web-site pop-ups?

Of course, there is no reliable evidence that manipulation occurs; nor that marketers believe manipulation is possible[18] or that consumers believe they are being manipulated. But there is a recent article in the *Harvard Law Review* that strongly asserts the opposite: It finds significant consumer manipulation.[19]

The article insists that "because individuals exhibit systematic and cognitive processes that depart from axioms of rationality, they are susceptible to manipulation by those in a position to influence the decision making context." Adding to their bleak picture of consumers' intelligence and lack of willpower, the authors argue that "because a multitude of non rational factors influence individual decision making, consumers cannot be expected to engage in efficient product purchasing analyses." Reduced to its bare essentials, the authors speculate that Americans have become puppets to sellers who cause them to buy products they don't, or shouldn't, want. Not surprisingly, the authors' solution is aggressive government intervention.

The article is worth reading, as it is in the *Harvard Law Review* and thus will be taken more seriously than it should. Undoubtedly, it will soon show up in privacy position papers and memoranda in governmental departments. As proof of the pudding, it may already have played a role in motivating US Attorney General Janet Reno to get further involved in the tobacco wars. The recent civil action by the Justice Department against tobacco companies strongly reflects the theory of the article.

The article, in any event, is wrong. Regardless of the volume of personal information that marketers use to fashion solicitations, manipulation of consumer purchasing decisions is extremely difficult in a competitive economy. For every

product offering that might entice a thoughtless, perhaps manipulated, decision, there are scores of others in different colors, sizes, shapes, packaging, and prices, each one luring the consumer away from the would-be manipulator. Competition, in short, creates a system of checks and balances where no one can have the upper hand with consumers for long, if at all.

It is a certainty that whenever a company, via data mining, discovers a predilection of a consumer, scores of others will soon make the same discovery, and still others will make their own discoveries about different predilections. For example, if I buy a pair of hiking boots from a department store with a credit card, both the store and card company may use the information to try to get me to make another, related purchase, say, of outdoor products. If I go on the Internet to search for hiking equipment and places to hike, still more solicitations might ensue. But because I am a complex, diversified buyer, hiking is only a modest fraction of my commercial decisions. I'll buy scores of other products and services that information magnets will capture and perhaps turn into still more solicitations. The evidence of these possibilities is in my mailbox every day: businesses checkmating each other and manipulating nothing. For all their efforts, I simply ignore their solicitations. I am in control.

In the near future, consumers will have even more control, thanks to smart cards and software that will make them all but anonymous at points of sale on and offline. Other software soon will make it easy for consumers to identify organizations that maintain information about them—retailers, employers, schools, health-care providers, and politicians—and get access to that information with an opportunity to correct what is erroneous. Powerful new tools, indeed, that the marketplace, not government, is providing. These tools will shift the balance of power in consumers' favor, so that by the middle of this decade, it is likely that the paranoia about being watched will mostly be on the institutional side: government and business.

Let's pause on this point: consumers snooping on businesses. If a consumer wants to find out about shoes at a department store, credit cards at a bank, hotels in Alberta, and so on, all she has to

do is go onto the Internet and ask the world. In a flash, she will get a massive amount of valuable information from other consumers, consumer advocates, government agencies, infomediaries, the media, competitors, and others, each cautioning her how to protect herself, how much to pay, what outlets to avoid, and the like. The Internet gives her unprecedented tools to eliminate guessing about brands and product quality.

In comparison, the information businesses gather about consumers' transactions, on and offline, is sketchy and at best enables little more than a solicitation crapshoot—a game against odds that they will contact the right person on the right day with the right offer and make a sale. And, of course, not make a contact in the wrong way and lose the consumer forever. In short, what the business community gets about consumers is crumbs. To suggest that consumers nevertheless need government protection seems excessive, except perhaps when the government is the culprit.

INTERNET SALES TAXES & PRIVACY

We know from the encryption debates that politicians often are of a mixed mind about marketplace tools that protect privacy. They like them up to a point, but they are starting to wonder whether too much privacy will diminish their ability to govern. This is especially so on the issue of taxation of e-commerce transactions. Tax-enforcement agents across the United States are fearful that consumers are going to use the Internet to try to avoid paying sales taxes.[20]

The majority of them—states, cities, counties, villages, *et al*., maybe 30,000 to 50,000 taxing jurisdictions in all—don't want to give up a penny. What many of them want is the creation of a national data bank to track e-commerce transactions of every kind: by price, item, place of purchase, place of delivery, etc. Their data bank will resemble the Federal Reserve or the bankcard associations' settlement systems, except for all the personal information it will collect and distribute to taxing authorities. Nothing of its kind has ever been created in the US. Whether their data bank can pass First Amendment muster remains to

be seen. Moreover, because of the Compact Clause in the US Constitution (Article 1, Section 10), the states probably cannot create the bank without the approval of Congress, which seems unlikely. The combination of a data bank and taxes makes it too hot to handle.

It gets worse. Several states want the credit-card industry to play a major role in the Internet-tax-collection effort. The reason is simple: credit cards pay for virtually all e-commerce transactions and card issuers capture relevant details of each transaction for billing purposes. Because the issuers have information the states need, the states want to involve them in the collection effort. The attraction for the issuers is the additional discount revenue they will make from settling billions of dollars of sales taxes, as well as the political allies they will make in legislatures on other matters of importance, like protection of their information-sharing practices.[21] This is another reason to treat privacy within the "penumbras" of the First Amendment. By rigorously keeping government out of the privacy picture, neither side will be able to make deals to subvert marketplace solutions.

Credit-card issuers would be fools to hop in bed with the tax collectors. In doing so, they will commit two serious errors. They will exacerbate the growing distrust that customers already feel about their information practices, and provoke a new distrust that they have sold out to the worst snoopers of all. Just as bad is the risk that politicians will abuse the relationship by using it to raise new taxes, knowing that the message will come from the card issuers and not themselves.[22]

Let's face it, governments constantly try to find ways to snoop on citizens to achieve objectives like collecting taxes, dealing with crime, imposing moral standards, distributing benefits, and the like. But when government does it, there is a difference in contrast to business information practices: there are no markets to balance or erase its egregious effects—no opt-in, no opt-out.

OPT-INS, OPT-OUTS

The opt-in/opt-out issue, of course, is at the center of the political debate about business information practices. One side

of the debate says the law should not allow businesses to share consumer information with third-party marketers without the consumer's written consent at the inception of their relationship. The other side says businesses should have the discretion to share the information, subject to the consumer's right at any time to opt out. In each case, disclosure is a presumed feature of the opt-in/opt-out right.

There are myths of sorts on both sides of the debate. All businesses seem to read from the same hymnal when the opt-in issue is on the table. They claim that mandating an opt-in will kill their marketing efforts, thereby increasing their costs and the price of their products. They add that without the freedom to use information, customer service will suffer dearly. Interestingly, few, if any, of them know for sure that an opt-in exercise will lead to those results, because they have never tested it. They just seem to assume that consumers will abandon them *en masse*. If this is so, it is odd that any business would want to be in that position, much less insist on the right to continue it.[23]

It is also odd that businesses believe they cannot find the words, and perhaps the incentives, to persuade their customers to collaborate with what in most cases is a good thing: information use that leads to bargains. If the business community is to carry the debate against restrictions on information practices, it must conduct opt-in experiments. Until it has empirical proof showing otherwise, it should stop arguing that the roof will collapse because of opt-ins. Who knows, businesses might even discover from the exercise that their information practices cost more than they are worth.

In any case, since it is highly unlikely that legislatures, including Congress, have the constitutional power to outlaw secondary use of transaction information by the private sector, the practice will continue to be legal. And because it is legal, the only question is how consumers with a concern can stop it. Keep in mind that most consumers do not show concern, or at least do not act on their concerns when given the opportunity. They ignore even the simplest opt-out procedures. Moreover, they almost never inquire about the information practices of the

companies or banks they do business with. In the face of this apathy and as if to manufacture concern, privacy advocates insist that affirmative action in the form of an opt-in is the only way to protect consumers.

The opt-in approach, of course, is not a norm in business practice or the law. And that begs the question: Should the law require it to resolve a dubious privacy issue? Why impose a signature requirement[24] when so much else of consumers' transactions happens without a signature?[25] If the use of information to market products deserves such treatment, then many other, more important, aspects of consumers' transactions should also be carved out to include a signature. As it is, something like this happens when a consumer transacts for a mortgage. Between the application date and closing, the hapless consumer can end up providing a score of signatures or initials on more than a hundred pages of documents that nobody in their right mind would ever read, much less be able to understand or justify. Twenty years ago the process was relatively simple and it worked, but today a kind of madness has taken over that only lawyers can like. The opt-in approach for privacy risks is taking us down the same path.

Maybe the business community should offer to accept an opt-in requirement if Congress in turn will reimpose an opt-in for class-action lawsuits. Rule 23 of the Federal Rules of Civil Procedure used to operate on an opt-in basis. Until 1966, each member of a class seeking money damages had to sign up to be included in the case. According to a recent Rand Institute study, the change in Rule 23 to what now is an opt-out standard caused the number of class actions to "multiply many times over."[26] One must suspect that some of the reason for the exaggerated demand for privacy legislation is because of all the business it will give to class-action lawyers. But if an opt-in requirement is to become part of the equation, Congress should be consistent and require it for class actions also.

OPT-OUT FLAWS

The opt-out argument likewise is flawed. It holds that businesses should have a presumptive right to use much of the

information they collect from a consumer until the consumer tells them to stop. Businesses prefer this approach because they believe, probably correctly, that the more information they have about large numbers of consumers, the better they will get at providing them with what they want.

Keep in mind that if a business provides an opt-out right at the inception of a relationship, that right arguably is simultaneously an opt-in right, because it gives the consumer exactly what an opt-in does: the ability to prevent the use of information from the start. Of course, this presumes: 1) a disclosure of the right, which many, perhaps most, businesses do not provide or provide only in gobbledygook; and 2) the consumer will read the disclosure, an unlikely event close to 100 percent of the time.

Privacy advocates argue that disclosures are an imperative of consumer protection. But are they really? Hasn't the daily drum beat of critical media, political, and academic coverage of business information practices inoculated almost everybody about what is going on? Don't most consumers know what to do, but simply not do it? How many of them ask a business up front, before a relationship or transaction ensues, if it will use their information for secondary purposes?

Of course, if the business admits it will use her information, a concerned consumer has many options. She can demand an opt-out before going forward, request a *quid pro quo* (*e.g.* a discount), walk away, pay with cash (or anonymously, if online), or accept that the information use will be harmless and perhaps even beneficial. But if she does nothing, in the case of most established businesses, the worst harm will be a few pieces of junk mail or telemarketing calls, each of which is easily resistible. The benefits, on the other hand, could be cheaper, customized products and better services.

Putting the burden on consumers to fend for themselves on information matters, without government intervention or lengthy disclosures, might seem harsh, but it is no more harsh a responsibility than what they already face when they shop. They know they must regularly ask about price, durability, perishability, safety, warranties, service, maintenance, size, weight, aesthetics,

returns, dispute mechanisms, and on and on. They know they pretty much live in a *caveat emptor* world that by and large serves them well. And they know they are not helpless. So what is it about information use that provokes so many demands for special, elevated protection by government? If consumers can fend for themselves on so much else—matters far more complex, risky, and important to them than the use of transactional information for marketing purposes—why not the same for information practices?

Why not let them freely determine how much privacy they want? That's what they do most of the time anyway. For most people, for example, their residence is their most cherished privacy retreat. Yet it goes without saying that some residences are more protective of privacy than others. Tenement apartments are less private than suburban homes, and the latter are less private than the modern castles of the rich. While the privacy ideal might be the castle, it should not be government's task to get people there. It is up to individuals to figure on their own how much privacy they want and how to get it. Most people, of course, don't give the ideal a second thought. They pragmatically tolerate that a nearby neighbor may occasionally overhear their spats or goofiness, because they know the invasion isn't worth a fuss. By the same token, when left to deal with most business information practices, most of them sensibly shrug their shoulders and move on to more important matters.

Pragmatism probably explains why most consumers do not opt out when a business gives them the chance. Consumers know that the risks concerning secondary use of their information are modest at best and that, in any event, trying to prevent all of them is probably impossible.[27] Consumers interact with too many organizations that capture, buy, and share their information.

On any given day, most consumers probably deal with a score of businesses on and offline that record various information about them: utilities, phone companies, retailers, manufacturers, banks, investment advisors, insurers, credit-card companies, magazines, plumbers, carpenters, restaurants, grocers, and on and on. Depending on how the consumer pays, others also

might capture the information, like merchant banks for card transactions, credit-reporting agencies, network providers, and the like. Noncommercial organizations on a daily basis often do the same thing—charities, schools, government, the dreaded Motor Vehicle Bureau, politicians,[28] *et al*. Still other organizations capture information without any interaction with the consumer.

It is no secret that some of them repeatedly trade the information with others, subjecting it to a kind of multiplier effect, where the information in theory might pass on and on many times before it loses its relevance. Recapturing it, much less trying to find out where it went, would be impossibly expensive and time consuming for even the wealthiest consumer—and quite frankly not worth the fuss, because, in the end, what happens to the information in most cases is rarely harmful to anybody.[29] Most of it in fact is never used, in good part because it is unusable. If every trade of information led to a solicitation, consumers would receive scores of junk mail and telemarketing calls every day.

Trying to stop information sharing before it commences likewise seems out of reach for most consumers. There is simply too much to stop, too many privacy practices to investigate: organization-by-organization, product-by-product, account-by-account, and disclosure-by-disclosure, each one written differently, but mostly all in gobbledygook. And then there is the enormous effort afterwards to monitor for results. Who has the time, and why expend it on what is mostly harmless in any event?[30]

The privacy police would have us believe that someone "live" in each of the established organizations we regularly deal with is snooping into everything we do in search of information to manipulate or harm us.[31] It is amazing that people fall for this. Today the snoopers mostly are algorithms that have been fashioned to slightly increase the existing slim chance that the organization using it might get a person to buy something, complain a little less often, make a donation, offer services, fill out a form, etc.

Sophisticated information algorithms have been used by the credit-card industry for a long time. Ten years ago the industry

was happy with a 2 percent response rate to the solicitations it shaped with the help of algorithms—about a billion such solicitations per year. In 1999, the solicitations exceeded three billion, but the response rate dropped to only 1 percent. It tells you something: Despite all the new information that is available and being used, it is mostly useless in increasing acceptance rates.

That most data gathering by most organizations is harmless doesn't mean that consumers shouldn't be told in disclosures about what is going on. But the trouble with disclosures is that consumers do not read them. There are too many disclosures to read covering too many aspects of their lives—about companies, products, services, labor practices, safety warnings, discrimination, costs, duties, fines, and the like, virtually all written in gobbledygook and lost amidst a plethora of other information. The problem is information overload: so many public and private notices that people have learned to disregard them. It is a stretch for anyone to say that for once, in the case of privacy, a new disclosure law will work. About the only thing it will accomplish is temporary removal of the issue from the politicians' backs.

SECURITY IS THE ISSUE

For most consumers the issue in the end is not opt in or out, junk mail, telemarketing calls, those mysterious web-site pop-ups that know who they are, or another disclosure law to ignore; it is whether somebody will get access to their information and steal from them. More than anything else, consumers want security against crime. And that means they do not want key information like their Social Security or bank account numbers, income, and the like to get into the hands of crooks, who might use it to borrow in their names or break into their accounts.

For the most part, this has not been a problem. Most established businesses have excellent security systems and rarely experience a breakdown. But when they do, they fix it quickly and provide a fair remedy for victims. Anything less and the market, especially the media, will punish them severely.

CONCLUSION

Let me conclude my observations about myths in the privacy debate by repeating my belief that we should trust the market to resolve the privacy issues that disturb us so much today. They are not unlike the problems that any new industry faces. To assume, as so many do, that information technology will bring us in only one direction—a world where businesses use information to manipulate consumers' economic decisions—is itself manipulative. By promoting fear it lays the groundwork to usurp important constitutional principles. Like it or not, if privacy is a First Amendment right, as *Griswold* insists, we have little choice but to defend it on our own, just like free speech. The First Amendment tells us we must be patient in areas where use of the freedoms it covers might take a long time to bear fruit. Accordingly, it denies us recourse to legislation to speed things up.

But that should not be cause for despair. Competition forces entrepreneurs to listen to consumer demands and supply what they want. Privacy demands cannot be an exception to that rule, regardless of the dire predictions of some privacy-legislation advocates. As it is, new inventions and processes are being tested and implemented every day by industry. There are only two things that can hold them back: 1) premature legislation that will shift the debate and initiative from the marketplace to the courts (where lawyers will work their alchemy); or 2) consumer disinterest. Polls, of course, show that consumers are very interested in protecting their privacy from information-technology intrusions. But when given the opportunity to mitigate the intrusions, only a small percentage of consumers takes action.

But that, too, should not be a cause for despair. It can mean a thousand things. For example, it can mean consumers lack motivation because they are confused about the risks, harms, and solutions; or because they trust that the marketplace or government will eventually set things straight. It is likewise possible that there is inaction because privacy is an enigma to so many people. It is in the eye of the beholder and can be defined, measured, shaped, priced, protected, traded, and discarded in any number of different ways. It comes in degrees. It is like free

speech; it has pluses and minuses, and succeeds best when left alone. If we leave it alone, privacy will be safe in America.

Notes

[1] For a comprehensive history, see Philippe Aries and Georges Duby, eds., *A History of Private Life*, 5 vols. (Cambridge, Massachusetts: The Belknap Press of Harvard, 1987).

[2] In *Two Treatises of Government* John Locke wrote that the "preservation" of private property is "the great and chief end…of men…putting themselves under government." (New American Library, 1963), p. 395.

[3] I would loosely define a homogeneous culture as one with a dominant religion, racial, or ethnic group that demands conformity with norms, customs, rituals, language, prejudices, castes, and the like. A majority of the countries of the world fit the definition, including many in Europe. Conformity, I would add, is an enemy of privacy, because it constantly requires submission to group standards via observation and sanction. The flip-side might be that multi-diversity protects privacy by fostering pockets of resistance—nonconformity via private, individual actions. If so, the US arguably is a much more privacy-oriented culture than it is given credit for.

[4] For example, the right to arrange the marriage of children in many cultures has been a private right of parents for centuries. The spread of liberal democracy because of trade, migration, and telecommunications technology has replaced it with the private right of offspring to make their own decisions. In short, new information undermined old information.

[5] For example, via separate rooms and beds for each member of a household in a privately owned home as opposed to a single room in a rented apartment. Wealth also enables greater leisure time to enjoy private possessions. Without space and time, privacy is an ephemeral right. What is often forgotten is that businesses constantly increase the opportunity for consumers to enjoy privacy by reducing the time it takes to conduct transactions. ATMs and PC banking, for example, have reduced to minutes what took hours not more than 15 years ago. The Internet has done the same thing by making shopping faster—and more private—than ever. The less time consumers have to spend transacting, the more time they will have for private actions, like reading a book, courting a friend, participating in the political process, hiding in the hills, etc.

[6] It is ironic that Europeans, who have been victimized so much in this century by pernicious governments, nonetheless trust the public sector more on matters of privacy than the business sector. This is in strong contrast to the US, where law reflects greater distrust of government.

[7] Privacy advocates most often point to the Fair Credit Reporting Act as a successful privacy-protection statute. Their affection for FCRA is strange,

for it allows massive trading of intimate, and often sensitive, consumer information for credit, insurance, marketing, and employment purposes. To listen to their current arguments against information sharing, one would think they would want to repeal FCRA or at least amend it to allow consumers to opt in. But they wouldn't dare, because FCRA has proven so successful. It is crucial to our economy. Among other things, it benefits consumers with the most efficient, egalitarian, lowest-priced credit system in the world. And it does this by what privacy advocates in other contexts would condemn as an invasion of privacy. Our credit-reporting system tells us we have less to fear about information sharing than the advocates would have us believe.

[8] 381 U.S. 479, 85 S. Ct. 1678, 14 L.Ed. 2nd 510 (1965).

[9] I am not unmindful that *Griswold* and its author are anathema to many scholars and political groups, who view the decision as reflecting more the personal politics of Douglas than sound constitutional jurisprudence. I would argue, however, that *Griswold* is a reality and that we should consult it to help us deal with our generation's privacy issues.

[10] For example, against identity theft and exploitation of children.

[11] *Griswold* upheld more than just the right of a doctor and Planned Parenthood to enable a married couple in Connecticut to receive contraceptives; it sanctioned the *business right* to sell the contraceptives and information about them. As such, *Griswold* not only told the state to stay out of the couple's bedroom but to stay out of the business transaction, treating both as private places protected by the Constitution. The Court did this despite significant public opposition at the time to liberalized distribution of birth-control products and services. There are parallels here to current privacy issues that reason, once again, for government not to interfere.

[12] One extreme of course is crime, and yet the Constitution is so distrustful of government that it allows the search and seizure of information about a crime only under strictly-defined circumstances. The Fourth Amendment prohibits "unreasonable searches" and requires a determination of "probable cause" before a search can begin. The Fifth Amendment adds a layer of protection, prohibiting forced self-incrimination or "deprivation of life, liberty or property without due process of law." Coming after the First Amendment, it is only natural that the Fourth and Fifth are so deferential to privacy protection, even for criminals.

[13] The argument that people need privacy-disclosure laws to enable informed self-reliance is attractive, but constitutionally suspect. The First Amendment doesn't allow government to force religions to tell us about their intimate standards and rituals or require newspapers to disclose their sources so that we can make more informed judgements about articles. So by what justification can privacy merit different treatment? If privacy is a First Amendment right as *Griswold* has held, government must butt out.

[14] Based on a long line of Supreme Court decisions, the First Amendment applies equally to the states through the Fifth and 14th Amendments.

[15] "Our fundamental right of privacy has been almost completely eroded by rapid advances in computers." Richard Wolf, "States Move To Protect Online Privacy," *USA Today*, January 20, 2000.
[16] But see Robert Samuelson, "The Internet and Gutenberg," *Newsweek*, January 24, 2000. Samuelson says railroads, air flight, automobiles, and TV grew just as fast and had as great an impact as computers and the Internet.
[17] The risks that business practices impose on people's privacy are no greater than risks they face from the assertion of other First Amendment rights. For example, free speech and free press often lead to abuses the law cannot resolve. Media bias or apathy can make or break the reputation of people, organizations, political movements, businesses, and the like. Their actions can have a costly influence on government action (regulatory & judicial), market determinations, cultural acceptances, etc. The Supreme Court's decisions on obscenity and abortion have been convulsive by any measurement, but defended in any event as the raw price we often have to pay to be free. What we don't like about any of these decisions we must deal with on our own and not through governmental protections.
[18] If marketers believed manipulation were possible, they wouldn't keep it a secret for long—it would show up in speeches at their trade conferences, in trade- and B-school literature, in discovery and testimony at lawsuits, etc. I have dealt with among the best marketers in American industry for almost three decades and never once heard the word. They would laugh at the charge.
[19] Jon D. Hanson & Douglas A. Kysar, "Taking Behavioralism Seriously: Some Evidence of Market Manipulation," 112 *Harvard Law Review* 1420 (May 1999).
[20] Only a small number of states welcome elimination of sales tax on Internet transactions—often to help promote a local high-tech industry.
[21] The morass here might turn out like the mess we have with political action committees.
[22] See *Review and Outlook*, "George's Web," editorial, *The Wall Street Journal*, January 28, 2000.
[23] Businesses are well-aware of public and private polling that shows strong consumer views in favor of the right to opt in. But there is insufficient polling to indicate how many consumers would exercise the right not to opt in or what would motivate them to opt in. Moreover, since we have no idea how much, if any, an opt-in requirement will add to the cost of transactions, we have to be suspicious about the accuracy of the polling.
[24] Many of the opt-in proposals would require a signature, initial, or check mark in a box to make them effective.
[25] For example, few, if any, credit-card companies require a consumer's signature to open a card account, even when credit lines can run in the tens of thousands of dollars. Consumers in turn can use their cards for mail order, e-commerce, and many in-store transactions for big-ticket purchases without ever signing anything.

[26] "Class Action Dilemmas" Executive Summary, Rand Institute for Civil Justice (1999), p. 1.

[27] In the near future, software and perhaps infomediaries will enable a measure of success here, perhaps against big companies, but it is questionable whether the effort will make a big difference in stopping information mining by small and unseen players. Short of legislative prohibitions against the information practices that exasperate privacy advocates—a seemingly impossible task for any legislature—the best thing for everybody to do is to continue to debate the issue and look for private solutions.

[28] An Internet site recently reported that "the two leading Republican presidential candidates, Sen. John McCain and Texas Gov. George W. Bush, have contracted with Aristotle Publishing (http://www.aristotle.org) to target web users by matching web browsing habits and web site sign-up data with actual voter registration records." There's a message here.

[29] If the sorting of benign information by machines is so harmful that government must erect a barrier around it, then why shouldn't government carry the protection a step further and apply it in other spheres? For example, should it require restaurants to have more space between tables to prevent diners from eavesdropping on each other? The point here is that privacy exaggeration can lead to a slippery slope, to paranoia that corrupts the smart use of law and citizen self-reliance.

[30] This is not to say that consumers should give up on the various tools that are available to them. It is just to recognize that they should be selective. Perfect privacy comes only in the grave. Privacy protection has always come at a price and can be very expensive for those obsessed about it. Those who desire impregnable fortresses to keep away the world will find it is impossible and ultimately lonely.

[31] Much of the privacy debate results from fear mongering—privacy advocates instilling images of voyeurism by live people, as though data workers were peering one-on-one into individual's windows, looking for information to embarrass them.