Policy Study 414
March 2013

Reason

It's Not Personal: The Dangers of Misapplied Privacy Policies to Search, Social Media and Other Web Content

By Steven Titch
Project Director: Julian Morris

Reason Foundation

Reason Foundation's mission is to advance a free society by developing, applying and promoting libertarian principles, including individual liberty, free markets and the rule of law. We use journalism and public policy research to influence the frameworks and actions of policymakers, journalists and opinion leaders.

Reason Foundation's nonpartisan public policy research promotes choice, competition and a dynamic market economy as the foundation for human dignity and progress. Reason produces rigorous, peer-reviewed research and directly engages the policy process, seeking strategies that emphasize cooperation, flexibility, local knowledge and results. Through practical and innovative approaches to complex problems, Reason seeks to change the way people think about issues, and promote policies that allow and encourage individuals and voluntary institutions to flourish.

Reason Foundation is a tax-exempt research and education organization as defined under IRS code 501(c)(3). Reason Foundation is supported by voluntary contributions from individuals, foundations and corporations.

Reason Foundation

It's Not Personal: The Dangers of Misapplied Privacy Policies to Search, Social Media and Other Web Content

By Steven Titch

Project Director: Julian Morris

Executive Summary

Millions of people have come to understand the Internet as a new media platform. For the government, unfortunately, basic comprehension of the business models and consumer demand that drive this platform remains elusive.

Traffic and usage statistics show the public is enthusiastically embracing the Internet as a two-way information medium. Facebook, the leading social network, says it reached 1 billion members in October 2012. But the traction other sites are gaining shows that interest in social networking is hardly plateauing. Pinterest, launched in March 2010, has reached 25 million U.S. users. Prognosticators are heralding it as the next Facebook.[1]

But while social media and other tools for consumer information-sharing on the World Wide Web speed ahead, lawmakers and regulators are doing everything they can to slow them down. Congress, the Federal Trade Commission and the White House itself, responding to concerns from privacy advocates, which include groups such as the Electronic Privacy Information Center (EPIC), Free Press and Consumers Union have been pressing for more government oversight of the way websites collect and use information that users provide—either directly through user interaction or indirectly through special programming embedded in Web browsers and websites.

Most of the free, Internet-based services that consumers take for granted are supported by advertising. At issue is the way websites collect and statistically analyze information to match advertising to users' interests. Nearly everybody agrees that consumers have the right to know what type of data is being collected, how it is being used, and, if they wish, the right to withhold this information, or "opt-out"—and the market has met this demand on its own. The government,

nonetheless, is contemplating more sweeping steps, such as those now advocated by the White House, for example the vaguely worded "Online Privacy Bill of Rights" that would place legally enforceable restrictions on how websites collect and use consumer information, pushing the U.S. toward a stricter regime akin to the European Union's Privacy Directive. If adopted, these restrictions could present a host of unintended consequences for consumers, websites, and the overall environment of the Internet, and potentially short-circuit the current Internet service environment where freely available information has become the norm.

Web advertising platforms are based on the mining and correlation of information that a user supplies to draw conclusions about the likes, tastes and purchasing tendencies of that individual. In a way, this is simply a refinement of techniques marketing and sales persons have used for decades, if not centuries.

In the offline world, most information collection and analysis is done in the background. Owners of small businesses, be they barber shops or bookstores, grow to know regular customers well enough to anticipate their needs. Larger companies, such as restaurant and supermarket chains, track sales of specific items and use the data to make decisions about purchasing and inventory, and even to tailor brands or menu items to local tastes. Because on the Internet targeting techniques can assert themselves quickly and dramatically—as in the form of directed advertising—some believe these information-gathering and analytics techniques to be an invasion of privacy and want to prohibit them or put steps in place to render them less effective.

These calls for regulation, however, fail to account for the benefits analytics have for users. Targeted and behavioral advertising techniques help consumers identify sellers and gain more information about products, prices and differentiators that much more quickly. In addition, targeted advertising results in a more cost-effective market. Sellers can identify and serve potential buyers faster and more effectively and avoid devoting resources to more scattergun approaches. These economic efficiencies help lower prices.

That's why legislation and policies to regulate or prohibit the consensual sharing, collecting, analysis and correlation of consumer information by websites will undermine Web commerce, consumer choice, a growing base of free entertainment and information services and applications, and lead to other consequences for consumers and U.S. competitiveness.

Websites can collect information in four principal ways:

- Directly from user input—that is, from information supplied by the user in subscription forms, interactive applications such as website polls, and, most recently, through information, preferences and "likes" on social networking sites like Facebook, Google+, and Pinterest.
- Through embedded software codes, called "cookies," that websites place on Web browsers like Microsoft Explorer, Mozilla Firefox, Google Chrome and Apple's Safari.
- Through "clickstream data," which record user activity on a website.
- Through user searches and Web browsing history.

All of this information has a role in supporting Web advertising. And just as with other media, advertisers need a way of measuring the effectiveness of their ad purchase. Whom is their ad reaching? Are these users the right targets? Is it leading to purchases?

Targeted and behavioral advertising isn't just something big companies like Google and Facebook do. It is a business model that serves as the foundation for most of the free or inexpensive Web-based information and entertainment users currently enjoy. The imposition of a top-down regime that limits the choice individuals have when it comes to sharing information would have serious, if not fatal, consequences for this model.

These proposed laws and regulations are being driven by genuine concerns about privacy and the loss of control some users feel when it comes to their personal information. Indeed, privacy laws are generally good when they protect individuals from theft and fraud, and in the process ensure the integrity of trusted systems—banking, health care, education and so forth. On the other hand, privacy regulation becomes troublesome when it tries to influence or change behavior, substituting the consumer's informed choice with the preferences of the government.

Unfortunately, that is the trend in much of the proposed regulation of search, social media and other websites that gather user data. Suggested solutions have fallen into several groups, and range from light to heavy in their degree of intrusion and coercion regarding consumer interaction with websites. Broadly categorized they are:

- Mandatory or optional Opt-in/Opt-out choices regarding the disclosure of certain information;
- "Do Not Track" legislation that prohibits websites from collecting user browser data regardless of whether consumers consent;
- Agreements between the government and major Web companies on user privacy and the collection and use of user data;
- Creation and enforcement of "Online Privacy Rights;"
- Outright privacy directives that regulate the collection and use of user data, as seen in the European Union.

Each of these approaches presents differing degrees of intrusiveness, but all presume to enforce a top-down, statutory regime. The problem is that technology does not lend itself to slow-moving, one-size-fits-all regulation, but instead thrives when best practices are allowed to bubble up from consensus. Best practices can also adapt as technology develops and user perceptions and habits change.

The establishment of online privacy "rights" is of particular concern because, as drafted by the White House, they are vague and, if legally codified, stand to short-circuit innovation and experimentation because of the compliance concerns they will raise. Furthermore, the White

House's privacy rights track closely with the EU's Privacy Directives, which evidence shows adversely affected advertising effectiveness. An analysis of the Web advertising market undertaken by researchers at the University of Toronto found that after the EU Privacy Directive was passed, online advertising effectiveness decreased on average by around 65% in Europe relative to the rest of the world. The authors go on to conclude that these findings will have a "striking impact" on the $8 billion spent each year on digital advertising: namely that European sites will see far less ad revenue than counterparts outside Europe.

As advertising revenues are slowed, so will the growth of sites that use the targeted ad model, which include services that are the most innovative and provide the most consumer value. An immediate consequence would be the decline of the number of free content, information and services available on the Web. Regulation would add a new compliance burden on any start-up hoping to use targeted ads, creating an obstacle that would affect capitalization requirements at best and kill the business model for free services at worst.

The "Mother May I?" nature of the regulation would pre-empt experimentation with different business models that would employ user information in new ways. This is a major risk of any regulation or legislation in technology, an area that is constantly changing and evolving, and where success and survival often hinge on out-of-the-box thinking.

Regulations against information-sharing also undermine the community-building character of the medium. One of the reasons people go online is to meet and interact others who share interests and passions. Individuals with unique interests—from bird-watching to numismatics to Axis & Allies gaming—can connect with far more like-minded individuals than they might in their own geographic community. These communities in turn build knowledge bases that the general population of users can turn to from time to time. The ripple effect of the proposed regulation would constrain this information-sharing as well, keeping people from using the Internet for the very capabilities that serve this population.

Finally, much of the privacy regulation being proposed is purely precautionary. It is based on speculative "what if" and "what might" scenarios that imagine potential harms but fail to identify any extant ones. Market forces, however, have already forged a powerful check when companies overstep what customers see as defined privacy boundaries. Although lawmakers find this trial-and-error process cumbersome, it is necessary because user attitudes regarding information-sharing are complex. There is a documented "privacy paradox," that is, multiple studies have found that while users express concern about the sharing and use of personal information on the Web, they go ahead and do so anyway. The only way websites are going to resolve this paradox is through experimentation. In the course of their testing, they are bound to overstep. When popular companies like Google and Facebook have done so, they have faced a rapid backlash from users that forces proper corrective action more swiftly and powerfully than could possibly be achieved by regulation. In each case, this has been followed by an apology and retrenching, and the companies have retained customer goodwill.

The privacy paradox notwithstanding, recent data suggest that users are aware of their privacy options and making use of them. Users appear willing to take responsibility for managing their own privacy preferences. A new study from the Pew Research Center's Internet & American Life Project, published in February 2012, found that a majority of social network site users (58%) restrict access to their profiles. Women are significantly more likely to choose private settings—only 20% said their main profile is set to be completely public. Women who use social networking sites are more likely than men to set the highest restrictions (67% vs. 48%).[2]

While half of social networking site users say they have some difficulty in managing privacy controls, just 2% said it is "very difficult" to use the controls. The balance—49%—said setting privacy controls was "not difficult at all."

Examination of the technology, business models and consumer research supports a light-handed approach to regulation of websites with regard to their collection and use of personal information. Technology moves too quickly for legislation to keep up. Entrepreneurs need to have freedom to explore new business models without looking over their shoulder for fear of a government objection. Finally, consumers show a willingness to exchange information about their tastes and lifestyles in return for the tangible value of free services.

The case for allowing free market models to shape the way consumers choose to interact with websites can be summarized in five points:

1. Top-down mandates slow technology innovation.

Legislative and regulatory directives pre-empt experimentation. Consumer needs are best addressed when best practices are allowed to bubble up through trial-and-error. When the lagging economic and functional development of European Web media, which labors under the sweeping, top-down EU Privacy Directive, is contrasted with the dynamism of the U.S. Web media sector, which has been relatively free of privacy regulation, the difference is profound. U.S. Web entrepreneurs continue to push the envelope in terms of creativity and innovation. Facebook, LinkedIn, Groupon, Foursquare and Pinterest are just a handful of popular sites that have emerged since 2004, just as the EU Policy Directive was taking effect across the continent. It is telling that no analogs to these ventures have arisen in Europe. Additional research shows that overall, the effectiveness of Web-based advertising is far lower for sites in Europe, where targeted advertising is regulated, than it is in the U.S.

2.Consumers push back when they perceive that their privacy is being violated.

Google and Facebook, two of the largest and most visible Web-based enterprises that collect user data, have felt user backlash on several occasions when they have changed their privacy policies or, in the eyes of users, disregarded them. In every case, the company reacted far more quickly than the government could. When the FTC did finally render judgment, it could find no harms

worthy of fines or sanctions. Just as important, despite their missteps, neither Facebook nor Google lost much in terms of user goodwill. Their CEOs apologized and promised to do a better job communicating privacy policy and any changes. They serve as excellent examples of how the market can correct itself when consumers express displeasure.

3. Web advertising lives or dies by the willingness of consumers to participate.

As a corollary to the point above, Web sites that derive revenues from targeted advertising must be sensitive to user perception because if users believe they have been exploited, they will stop visiting the site. MySpace is an example of a social network that once dominated its space. But its reputation as being a largely unsupervised community for teens, its troubling susceptibility to phishing, malware and spam, as well as (overblown) reports of its being an easy source of pornography and a haven for child predators were ultimately fatal. In early 2008, MySpace was still the most visited website in the world. As of March 2012, MySpace ranked 160th on Alexa, another Web metrics site.[3]

4. Contractual arrangement allows customers to customize their unique privacy wishes.

Privacy concerns are best addressed through clear policies and contractual agreement. Well-crafted legislation can endorse this, yet still leave room for users to set their own privacy parameters in line with their own preferences.

Privacy policies can be enforced via the FTC or the courts, the latter being preferable. This process has worked well in the area of information security, and courts have found retailers such as T.J. Maxx and banks such as Belmont Savings Bank in Massachusetts liable for consumer loss because of data breaches. Opt-in, Do Not Track and privacy bills of rights are all about substituting government mandates for individual discretion. They do not strengthen or expand on any current laws against online fraud or theft, which by themselves are quite strong.

5. Greater information availability is a social good.

An unfortunate aspect of the call for privacy regulation is the *a priori* assumption that commercial information-gathering and targeted advertising are questionable practices from which consumers need to be protected. On the contrary, information-gathering in all areas of market research, but certainly audience research in media, has a long history. Consumers are willing to provide information about age, gender, income, lifestyle, preferences and tastes in return for more streamlined and customized information about products and services which might interest them, as long as they are satisfied that the information they provide will be confidential or anonymized.

There are wider social benefits when more information is available to buyers and sellers. For one, limited resources can be allocated better. Suppliers can know which regions of the country will

have the greatest demand, and adjust their distribution networks to meet it. Product goes to where it's most needed; better value is derived from transportation costs, and there is less waste. These are just basic examples. Multiplied across global markets and applied to hundreds, if not thousands, of information parameters and variables—all processed at very low cost—fosters productivity and wealth throughout the economic ecosystem. This is why it's best to derive privacy policies from a strong and constantly evolving knowledge base of best practices, rather than to codify them into laws that, in their government's failure to foresee innovation, will unintentionally preclude it.

Table of Contents

Part 1

Introduction

Millions of people have come to understand the Internet as a new media platform. For the government, unfortunately, basic comprehension of the business models and consumer demand that drive this platform remains elusive.

Search engines have evolved to the point where they can deliver a precise answer to a user query within seconds, complete with content summaries, subcategories, and where pertinent, addresses, phone numbers, maps, images and customer reviews. Meanwhile, social networking has become a predominant communications tool for individuals to stay up-to-date with family, friends and acquaintances.

Elsewhere, more-specialized websites connect people with similar interests, hobbies and passions, creating communities where information and knowledge are shared and increased.

Traffic and usage statistics show that the public is enthusiastically embracing the Internet as a two-way information medium. Facebook, the leading social network, says it reached 1 billion members in October 2012. But the traction other sites are gaining shows that interest in social networking is hardly plateauing. Pinterest, launched in March 2010, has reached 25 million U.S. users. Prognosticators are heralding it as the next Facebook.[4]

But while social media and other ways of information-sharing on the World Wide Web speed ahead, lawmakers and regulators are doing everything they can to slow them down. Congress, the Federal Trade Commission and most recently the White House itself, responding to concerns from privacy advocates, which include groups such as the Electronic Privacy Information Center (EPIC), Free Press and Consumers Union, have been pressing for more government oversight of the way websites collect and use information that users provide—either directly through user interaction or indirectly through special programming embedded in Web browsers and websites.

Most of the free, Internet-based services that consumers take for granted are supported by advertising. At issue is the way websites collect and statistically analyze information to match advertising to users' interests. Nearly everyone agrees that consumers have the right to know what type of data is being collected, how it is being used, and, if they wish, the right to withhold this information, or "opt-out." The government, nonetheless, is contemplating more sweeping steps, such as those now advocated by the White House, for example the vaguely worded "Online Privacy Bill of Rights" that would place restrictions on how websites collect and use consumer

information, pushing the U.S. toward a stricter regime akin to the European Union's Privacy Directive. If adopted, these restrictions could present a host of unintended consequences for consumers, websites, and the overall environment of the Internet. They would potentially short-circuit the current Internet service environment where freely available information has become the norm.

Web advertising platforms are based on the mining and correlation of information that a user supplies to draw conclusions about the likes, tastes and purchasing tendencies of that individual. In a way, this is simply a refinement of techniques marketing and salespeople have used for decades, if not centuries. The best salespeople have always worked to develop a relationship with their customers, making it a point to know facts about family, birthdays and personal preferences—all the better to anticipate that customer's needs. What the Web has done, however, is exponentially increase the amount of information available while reducing the cost of both its acquisition and the application of statistical analytics. These factors have been effective enough at matching advertisers to prospective customers that users are genuinely startled. Indeed, on one hand, consumers are concerned that marketers are exploiting the ease at which they can gather personal information, and groups such as EPIC have picked up on this to advocate for regulation. On the other hand, despite their vocal concerns, users willingly continue to provide websites with information about themselves, to the point where search and social networking are significant growth businesses. This "privacy paradox," which has been documented in several studies over the past ten years, complicates Web-based commercial relationships and is another reason regulators should go slow.

In the offline world, most information collection and analysis is done in the background. Owners of small businesses, be they barber shops or bookstores, grow to know regular customers well enough to anticipate their needs. Larger companies, such as restaurant and supermarket chains, track sales of specific items, and use the data to make decisions about purchasing and inventory, and even to tailor brands or menu items to local tastes. Because on the Internet targeting techniques can assert themselves quickly and dramatically—as in the form of directed advertising—some believe these information-gathering and analytics techniques to be an invasion of privacy and want to prohibit them or put steps in place to render them less effective.

These calls for regulation, however, fail to account for the benefits analytics have for users. Targeted and behavioral advertising techniques help consumers identify sellers and gain more information about products, prices and differentiators that much more quickly. In addition, targeted advertising results in a more cost-effective market. Sellers can identify and serve potential buyers faster and more effectively and avoid devoting resources to more scattergun approaches.

That's why legislation and policies to regulate or prohibit the consensual sharing, collecting, analysis and correlation of consumer information by websites will undermine Web business, consumer choice, a growing base of free entertainment and information services and applications, and lead to other detrimental consequences for consumers and U.S. competitiveness.

Part 2

Ways Websites Gather Information

To truly understand the aim of privacy regulations and the consequences they might have, it helps to understand how users supply information to websites, and how these techniques have evolved over the years.

Websites can collect information in four principal ways:

- Directly from user input—that is, from information supplied by the user in subscription forms, interactive applications such as website polls, and, most recently, through information, preferences and "likes" on social networking sites like Facebook, Google+, and Pinterest.
- Through embedded software codes, called "cookies," that websites place on Web browsers like Microsoft Explorer, Mozilla Firefox, Google Chrome and Apple's Safari.
- Through "clickstream data," which records user activity on a website.
- Through user searches and Web browsing history.

All of this information has a role in supporting Web advertising.

From the entrepreneurial perspective, the Web has always been seen as an advertising medium. In the first decade, the Web ad model mimicked that of print and broadcast. A website marketed itself directly to potential advertisers, selling "banners" and "buttons" the same way newspapers sold one-page and half-page ads and broadcasters sold 30- and 60-second ad slots.

Still, advertisers needed a way of measuring the effectiveness of their ad purchase. Whom was their ad reaching? Were these users the right targets? Was it leading to purchases? What other information could the website report about its audience? Newspapers and magazines provide advertisers with audited circulation data and can break down readership measurements based on age, sex, location, income and a host of other variables. Broadcasters use Nielsen ratings, plus their own audience research, to supply advertisers with similar data.

User Input

Active user input is the most obvious way websites collect audience information. Just by choosing to visit a site, a user provides a degree of data about him- or herself. For example, a visitor to the *Parents* magazine site, www.parents.com, is likely to be a parent (or an expectant one). A visitor to Travelocity.com likely is thinking about taking a trip. So simply by choosing to use the Web as an information resource, the user is volunteering to disclose personal information about herself and her interests.

But that data still might be too general for advertisers. How many people stumble on parents.com by mistake and never come back? How many Travelcity.com visitors are simply fantasizing about a vacation but lack the budget or time to take one? So the site, in return for offering visitors access to more specific information, such as airline fares or hotel rates, might request more personal information, such as date of birth, occupation, level of education and income. Elsewhere on the Web, publication sites will ask users to fill out a subscription form that might seek more demographic data. For the user, the incentive to provide the information is free access to magazine articles or to a valuable time-saving service, such as a side-by-side list of air fares.

Yet electronic questionnaires can be cumbersome and time-consuming and sometimes users don't want to fill them out. So in order to understand their audience better, websites also use cookies.

Cookies

A cookie is a short line of software code that assigns a specific ID to a browser when it connects to the website. The cookie is stored in the browser application on the user's device. Cookies allow a website to accurately determine its number of new and returning visitors. This is important because it provides context for the raw numbers of visits, or "impressions," a website can report. For example, a website that claims 10,000 impressions a day may sound like it has a large following. But cookies can determine how many of those visitors are unique, how many pages they view, and how often they come back. Cookies generally correlate their identifier with the device's IP address. But sometimes the cookie will incorporate information the user provides in a short form, such as name, email address and zip code, and maybe a few other preferences. In return, the user might get some additional value in the form of customized information instead of seeing a generic welcome page. For example, AccuWeather.com's cookie will customize weather information based on the user's location. Travel sites will display air fares from the user's home city.

On e-commerce sites like Amazon.com, cookies support familiar "shopping cart" functions. In this case, the cookie lets the site match your ID to the items you add to your cart. If you log off the site and come back later, the ID in your cookie tells the site to search its database for your cart. Here, the benefit of the cookie is a quick, convenient on-line shopping mechanism.

The way cookies work is often misunderstood. The personal information they contain is not retained by the website. In fact, it remains embedded in the user's browser program; the site just reads and processes it each time the user visits. Cookies do not record and send information users provide to other Websites. Neither do they collect, store and transmit information from other programs and applications on the user's computer, such as email, contact lists or software like Quicken.

Some cookies, however, do track user Web surfing and use that history to build a profile of user interests. By providing that data to another website, that site may be able to target ads better, or sell that information as research to other marketers looking to reach prospects with a certain set of interests. There is some debate whether these more sophisticated programs should be called cookies at all. Avi Goldfarb and Catherine E. Tucker, in a paper on Privacy Regulation and Online Advertising, place these codes in a separate category called "web bugs."[5] On the other hand, other authors conflate these types of cookies with spyware and malware, and consider them "malicious,"[6] even though they do not store information that personally identifies the user and, in the end, are used mainly to crunch the collected information into statistical models. This differs from spyware and malware, which indeed are used by unscrupulous sites and outright criminals, to plant viruses or steal secure information, such as usernames and passwords. While privacy matters overlap, fighting spyware and malware are security issues, which, in the discussion of e-commerce, should be considered separate from the collection of information for marketing. In marketing, information that's gathered is generally anonymized before it's analyzed.

Of course, the user has the option to erase cookies at any time, although this will delete any preferences and settings the user has with the sites that placed those cookies. The function is easily found in the browser's pull-down menus. Users can also set their browsers to reject cookies or, with each new site visit, give them a choice of whether to accept a cookie from that site. Spyware and malware, however, generally need to be attacked via security and anti-virus software specifically designed to find and delete them.

Clickstream Data

In addition to cookies, websites have developed one more source of information on visitors—clickstream data. Clickstream data tells a website what specific pages on the site the user views, how long the user spends on each webpage, the visitor's navigation path through the site, including first and last pages visited, the visitor's IP address, and the webpage the user viewed immediately before arriving at the website.[7] If the user found the site through a search engine, clickstream data can identify which one. It can identify the country of origin and ISP domain. As with cookies, any personally identifiable information is anonymized before processing.

The Role of Search Engines

Search engines add another facet of information-gathering because they can use search keywords as another tool to deliver, or "serve," advertising. When users type in the keyword "shoes" on a search engine, they will see a list of sponsored links for websites or brick-and-mortar stores that sell footwear. Moreover, even if a user does not click through to one of these listed sites, she may continue to see banners and buttons for footwear sites on the sites she visits thereafter.

This represents two dynamics at work. In the first instance, the search engine itself is serving ads based on the keyword or keywords used. In the second case, the search engine is employing the user's search and browsing history to target ads that it believes will interest her.

From their introduction in the mid 1990s, search engines have been trying to build their revenue model around targeting ad results based on user keywords. Although not the first search engine, Google is generally credited with significantly advancing search engine programming, algorithms and analytics to the point where the model is viable. Its success here has been the prime reason it has surpassed its predecessors to become the most popular search engine among users and the leading search engine in terms of ad revenue.

Furthermore, Google effectively democratized Web advertising by placing Web analytics in the hands of small Web publishers, bloggers and videographers. At first, only websites with significant resources could take advantage of cookies and clickstream data, because the process required a significant amount of custom software that called for skilled programmers. Through a series of acquisitions plus in-house work, Google now offers small, even part-time, Web entrepreneurs the necessary code to serve, track and measure Web ads—for free.

The Google AdSense and Analytics features allow a solitary blogger to cut and paste a string of software code into her site's underlying programming code to accept targeted advertising. If the blog becomes successful, this advertising can become a significant source of revenue. (There have been a number of stories of individuals becoming wealthy through a similar set-up on Google's YouTube video service.)[8] But even if traffic never reaches the level where it generates enough for someone to quit a day job, it can offset costs of operating a site, and there is no investment at the front end. Targeted ads are not limited to megacorporations. Without it, many of the small but significant sites that provide local news, divergent viewpoints, specialized information or simply fun content would not exist.

The Role of Social Networking

Social networking sites like Facebook pull user input back into the picture, bringing the process full circle. On social networking sites, users provide greater amounts of information about their preferences, likes and dislikes, location and activities. Their participation provides even more accurate data about a potential audience than search engines and Web tracking as there is less "guesswork" for analytic systems to do. If a Facebook user says she likes being at the beach, retailers of sunglasses and beach apparel know immediately without interpreting it by crunching browser data. Advertisers also can create Facebook pages, and both track ad effectiveness and gain insight into market demographics through tools such as the "Like" button. Again, this information is all voluntarily provided by the consumer, often in return for product news, coupons, special advance offers and other incentives.

These platforms are so effective that other Web companies are springing up with variations of the theme. Groupon (founded 2008) offers online coupons that help businesses better target consumers interested in their product. Foursquare (founded 2009) combines social networking with mobility. Yelp (founded 2004) combines search, directory services and location tracking to help consumers get immediate directions to—and comments about—nearby businesses, be they gas stations, hardware stores or coffee shops. Pinterest (founded 2009), which describes itself as an online pinboard, integrates social networking with photos and video in a way that allows users to organize design ideas, wardrobe options, gourmet cooking and any other concepts with a strong visual component.

This proliferation of user-friendly sites shows the ingenuity of Internet entrepreneurs in an unregulated Internet environment. But even more importantly, it gives a small glimpse of the successful infrastructure that would be affected—to the detriment of both operators and users—if the government decides to regulate the way search engines, social networking and other websites collect and use consumer information. All of these services, which provide immense value to consumers for free, are possible because users make the decision to provide information about themselves, their preferences, their tastes and location. Even as lawmakers have debated targeted advertising and other forms of data-gathering over the last few years, the model itself has become so embedded in the Web commerce ecosystem that any regulation can't help but risk serious disruption. The table below shows a small fraction of popular—and free—websites that rely on the targeted online advertising.

Targeted and behavioral advertising isn't just something big companies like Google and Facebook do. It is the foundation for most of the free or inexpensive Web-based information and entertainment users currently enjoy. The imposition of a top-down regime that limits the choice individuals have when it comes to sharing information would have serious, if not fatal consequences for this model.

Some Examples of Free Services Supported By Online Advertising			
Service	Website	Service	Website
Video	Hulu	Dating	Match.com
	YouTube		eHarmony
Weather	Accuweather		OkCupid
	Weather.com	Travel	Expedia
	Wunderground		Travelocity
Email	Gmail		Hotels.com
	Yahoo!		Priceline.com
	MSN	Music	Pandora
Calendars	Google		Live365
	Yahoo!		Jango
	MSN	Information websites	HowStuffWorks.com
	Keepandshare.com		About.com
Maps	Google Maps		WebMD
	Mapquest		Internet Movie Database
Translation Services	Google Translate	Blogs	HuffingtonPost
	Yahoo! Babel Fish		DailyKos
	Babylon		HitFix
Online Dictionaries	Merriam-Webster.com	Employment Listings	Monster.com
	Freedictionary.com	Product ratings and pricing	CNET
	UrbanDictionary.com		Ratings.net
Games	FreeOnlineGames.com	Newspapers	*New York Daily News*
	Miniclip.com		*New York Post*
	Pogo.com		*Los Angeles Times*
			Chicago Tribune
			Columbus (Ohio) Dispatch
			Houston Chronicle
			USA Today

Part 3

Privacy Legislation and Regulation

The widespread availability of free content and services on the Web, as well as the popularity of search and social networking applications are supported by an ecosystem of targeted and behavioral advertising. And yet, state and federal legislators, state attorneys-general, and federal agencies such as the Federal Trade Commission argue that websites that gather data from users, either directly through information and preferences consciously provided by consumers, or indirectly through website visits and search, pose a significant threat to their privacy.

These proposed laws and regulations are being driven by genuine concerns about privacy and the loss of control some users feel when it comes to their personal information. Indeed, privacy laws are effective when they protect individuals from theft and fraud, and in the process ensure the integrity of trusted systems—banking, health care, education and so forth. On the other hand, privacy regulation becomes troublesome when it tries to influence or change behavior, substituting the consumer's informed choice for the preferences of the government.

Unfortunately, this is the trend in much of the proposed regulation of search, social media and other websites that gather user data. Suggested solutions have fallen into several groups, and range from light to heavy in their degree of intrusion and coercion regarding consumer interaction with websites. Broadly categorized they are:

- Mandatory or optional Opt-in/Opt-out choices regarding the disclosure of personal information;
- "Do Not Track" legislation that prohibits websites from collecting user browser data regardless of whether consumers consent;
- Agreements between the government and major Web companies on user privacy and the collection and use of user data;
- Creation and enforcement of "Online Privacy Rights" by the Executive Branch;
- Outright privacy directives that regulate the collection and use of user data, as seen in the European Union.

Opt-In/Opt-Out

These bills have a wide scope. For example, the New York State Assembly's "Online Consumer Protection Act," introduced in February 2011, would have established new online privacy rules and required marketers to allow consumers to opt out of any information collection for purposes of online behavioral advertising, but ultimately was defeated.

These bills however, were less intrusive because they don't try to alter the way social networks function or do business. They recognize that customers have a right to withhold personal information, a fact that the industry does not dispute. Still, as the information users share becomes more varied in its degree of sensitivity, a single opt-in/opt-out setting, which most of these bills call for, might prove too general. Indeed, Facebook offers a considerable number of opt-in choices for various types of information, such as status updates, photos, activities and likes. Between browser options that let users reject cookies and the menu of opt-out options websites currently offer, the market is perhaps responding faster and more qualitatively than legislators to user privacy concerns.

While the New York bill may have simply been redundant, other opt-in bills have been flawed. California's ill-conceived Social Networking Privacy Act, defeated in May 2012, would have required social networking sites to default to "no information-sharing" for all new members. Given that the motive for joining social networking sites is to share information about oneself, demanding that these sites make such sharing impossible at the outset seems counterproductive and belies a basic misunderstanding on the part of lawmakers as to what social networking is all about.

Do Not Track

Due largely to an increase in privacy controls on social networks and more transparent privacy policies by websites, interest in Opt-in/Opt-out bills faded by the end of 2011. They were replaced, however, by an uptick in so-called "Do Not Track" bills aiming to regulate the collection of browser information, such as that used by cookies and in clickstream data, that is critical to targeting Web ads.

In Congress, Sen. Jay Rockefeller has introduced a "Do Not Track" bill that would regulate how social networking, search and other e-commerce sites gather and use information. This bill reflects similar legislation in various states that would force sites to either stop gathering information or offer extensive opt-in procedures.

The Rockefeller bill would require the FTC to promulgate regulations that establish standards for implementing a mechanism whereby individuals can "simply and easily" indicate whether they want online service providers to collect personal information, and prohibit service providers from collecting personal information on users who have expressed a do-not-track preference. Nonetheless, service providers would still be allowed to collect personal information when

necessary to provide a requested service, as long as the information is then anonymized or deleted, or if the individual receives clear notice and provides consent.

The Rockefeller bill would authorize the FTC to determine which providers of online services are required to comply with the Do Not Track rules, as well as interpret what personal information would be covered by the regulations.

Violations would be considered unfair or deceptive practices under the FTC Act. The bill would also empower state attorneys-general to bring civil suits, with a cap of $15 million for all civil penalties against a person who violates a rule.

The problem with this bill—and this is a continuing theme in privacy regulation—is its vagueness. It does not define personal information, nor does it state the specific harms it seeks to prevent or redress. It leaves the FTC with the open-ended job of defining offenses on an arbitrary case-by-case basis. This builds in a troublesome "ex post facto" element, in that companies won't know they've violated the law until the FTC decides that they did.

But considering the various types of data websites gather, the definition of personal information and the identification of harms are critical to any privacy regulation going forward. That the Rockefeller bill punts them both to the FTC is symptomatic of lawmakers' failure to appreciate consumers' desire for choice in what they wish to disclose and the privacy paradox in general.

The bill is also contradictory. While attempting to place restrictions on the way websites use information, it acknowledges that such information is necessary for the site to provide services. The Rockefeller Bill wants to have its cake and eat it, too. As noted in the earlier section, AccuWeather's cookie lets the user see the temperature and forecast for his home location. Does that make AccuWeather's cookie necessary to providing its service, as opposed to another website's cookie that simply passes on user data but makes no difference in how the site presents itself to the user? Does that mean every website will have to justify its use of cookies? And what exactly constitutes personal information? Is it religion? Income? Occupation? Hobbies? Favorite baseball team? Just contemplating the potential regulatory headaches that arise when cookies are considered, let alone clickstream data or information the user provides by choice, should give lawmakers pause. And through all this, the bill forgets two key features that all browsers now have: "Delete Cookies" and "Do Not Track."

Users have considerable control over what they choose to share online. They are in the best position to decide for themselves what information is too personal to share. It is a far better solution than creating a regulatory structure around what are, at the end of the day, comfort points that differ with each individual.

FTC Settlement with Facebook, November 2011

In December 2009, 15 privacy groups filed a complaint with the FTC seeking an investigation over possible deceptive trade practices on the part of Facebook pertaining to its privacy policy and its use of user information.

The resulting FTC complaint[9] listed a number of instances in which Facebook allegedly made promises that it did not keep:

- In December 2009, Facebook changed its website so that certain information that users may have designated as private—such as their Friends Lists—was made public. The FTC said Facebook should have sought user approval in advance or, at very least, warned users that this change was coming.
- The FTC said Facebook suggested that third-party applications that users installed would have access only to user information that the applications needed to operate. In fact, the apps could access nearly all of users' personal data—data the apps didn't actually need.
- Although Facebook told users they could restrict sharing of data to limited audiences—for example with "Friends Only," the FTC said selecting "Friends Only" did not prevent user information from being shared with third-party applications their friends used.
- Facebook said it had a "Verified Apps" program and claimed it certified the security of participating apps. The FTC claimed it did not.
- Facebook maintained that it would not share users' personal information with advertisers. The FTC alleged it did.
- Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible. According to the FTC, however, other Facebook users could still view these pictures and videos after the original users had deactivated or deleted their accounts.
- Facebook claimed that it complied with the U.S.-EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union. The FTC claimed it didn't.

The ensuing settlement, finalized in November 2011, barred Facebook from making any further deceptive privacy claims, required that the company get consumers' approval before changing the way it shares their data, and requires that it obtain periodic assessments of its privacy practices by independent, third-party auditors for the next 20 years.[10]

Specifically, under the proposed settlement, Facebook is:

- barred from making misrepresentations about the privacy or security of consumers' personal information;
- required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences;

- required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;
- required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers' information; and
- required every two years for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected.

The main takeaway in this is that, despite more than a year of investigation, the FTC did not find Facebook guilty of any significant wrongdoing. It issued no fines or sanctions against the company or its officers and in the end simply demanded that it perform third-party auditing for the two decades. As for the privacy policy requirements, Facebook implemented all of those shortly after the initial complaints, months before the FTC wrote them into the settlement. In the wake of the settlement, Facebook founder Mark Zuckerberg admitted that the company had made some poor decisions regarding user information but emphasized a renewed commitment to the company's respect for the personal information of its users.[11]

FTC Settlement with Google, March 2011

The FTC's Facebook settlement followed its March 2011 settlement with Google regarding the search engine's Buzz social networking service. Although Buzz never took off, the settlement, like Facebook's, required the search giant to develop a comprehensive privacy program and submit to two-year independent privacy audits for the next 20 years.

In its report on the settlement,[12] the FTC pointed to alerts Google used to enroll users in Buzz. On the day Buzz was launched, Google Gmail users got a message announcing the new service and were given the option to enroll or decline. The FTC said that some users who declined were nonetheless enrolled in certain Buzz features. Those who opted-in, according to the complaint, were not adequately informed about how their information would be used. Google's "Turn Off Buzz" option also did not fully remove users from the social network, the FTC said. According to the FTC, this violated Google's own privacy policy.

Again, as with Facebook, the FTC stopped short of seriously sanctioning Google, hitting it instead with the same 20-year audit requirement as Facebook, a resolution that suggests that the agency, finding no wrongdoing, felt the need to "do something" to justify the time and resources spent on both investigations.

As wasteful as these investigations might have been, the ultimate lack of punitive action is evidence that while Facebook and Google both skirted their privacy policies, the FTC, in the end,

concluded that no serious harm was done to consumers. What the agency clearly wants is transparency, which both Facebook and Google seem willing to provide. The encouraging aspect is that, while attempting to hold the companies to their stated policies, the FTC was leery of punishing experimentation. Both Facebook and Google were trying to create innovative products and services when they tripped up. In these two settlements, the FTC signaled that it might be better to tolerate the occasional privacy overstep over creating an enforcement regime that would strangle new ideas in the crib. Rather than give the FTC more power to take pre-emptive regulatory action, Congress and the White House should pause and absorb the message current commissioners are sending.

On-Line Privacy Bill of Rights

Yet despite the FTC's restraint and the industry's self-regulation, as seen in the adoption of more transparent privacy policies and "do not track" browser settings, the White House chose to double down on privacy regulation, and on Feb. 22, 2012, issued what it terms an "online privacy bill of rights."

White House Privacy Bill of Rights

Here are the seven rights that the White House is calling for:

1. **Individual Control:** Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
2. **Transparency:** Consumers have a right to easily understandable and accessible information about privacy and security practices.
3. **Respect for Context:** Consumers have a right to expect that companies will collect, use and disclose personal data in ways that are consistent with the context in which consumers provide the data.
4. **Security:** Consumers have a right to secure and responsible handling of personal data.
5. **Access and Accuracy:** Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
6. **Focused Collection:** Consumers have a right to reasonable limits on the personal data that companies collect and retain.
7. **Accountability:** Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the consumer-privacy bill of rights.

For all the good intentions it expresses, the "online privacy bill of rights" is a bad idea. First, it confers the status of "rights" on what should be truly labeled guidelines or best practices. Rights connote an absolute. Guidelines and best practices connote flexibility for adaptation to changing conditions, which is precisely the environment in which Internet enterprises operate.

The term "rights" also carries the implication of top-down imposition. But technology does not lend itself to statutory regulation. Instead, best practices are developed through bottom-up consensus and trial-and-error. The White House seems willing to give lip service to this idea by suggesting a "multi-stakeholder process" to arrive at sound privacy policies. How this process will work, who will participate and who the final arbiter will be is left unsaid. However, by injecting

the loaded word "rights" into the dialogue, the White House signals it believes that government should have the final word.

If approached as guidelines or best practices, the seven "rights" the White House outlines are not intrinsically bad. With the force of law behind them, however, they become troublesome because their language is so vague. The first "right," for example, gives consumers control over how companies use the personal information they collect. Again, we are presented immediately with the challenge of defining "personal information." If interpreted broadly, does this mean no website can use any browser information without user consent? Will the user be tasked with submitting a permission form each time he visits a new site? If a website develops a new way of using user information to provide greater value, does it have to seek opt-in from every user? If it chooses to change the presentation of user data, such as Facebook did with its controversial introduction of Timeline, does it need government permission? The answers will depend on who's in charge of the FTC at the moment. There is every reason to expect decisions will be capricious, arbitrary and fluid over time.

Especially problematic are "rights" three and six, which would require websites to use data only in the context it was provided and impose limits ("focused collection") on the data companies can collect and retain.

Once more the language is vague. The context rule can be interpreted to mean that a company cannot use any customer data other than to support the service or application for which the data was requested. In an aggressive privacy enforcement regime, that might mean that if a customer visiting ESPN.com wants to navigate to the NCAA page, ESPN would be forbidden to use that navigation information to deliver anything but the latest college sports news and scores. Passing that data on to a third-party, which might use it to serve an ad for team merchandise, could be construed as outside the user's context. Likewise, amalgamating that user's navigation information with data from the millions of other visitors to ESPN.com, even if it's anonymized, may also be considered non-contextual use.

Similarly, the idea of focused collection attempts to tell companies how they can apply the user data they collect to other parts of their enterprise. Cookies, as we've shown, tell a website owner how often a user returns to the site. Clickstream data tell the owner how long the user stays and which pages he accesses. This provides feedback as to how well the content is retaining loyalty, and if loyalty falls off, where changes need to be made. But a rule that would require websites to expunge user data after a specific length of time, even if it were as liberal as 12 months, would hurt the site's ability to react to long-term shifts in customer habits.

These two examples illustrate the overarching problem with the Online Privacy Bill of Rights, as well as any other effort to impose rules on the collection and use of information, which is simply this: *The use of information is impossible to regulate.*

The Online Privacy Bill of Rights conflicts with the fundamental right of free inquiry. Once a piece of information has been discovered, documented or deduced—it's out there for use by anyone who finds it relevant to his research. The context in which that information, or the data that underlie it, was originally collected is immaterial. An individual may have paid his electric bill in the context of compensating the electric company for service, but the electric company can use that information to track usage and revenue patterns for a given area. Further, if the electric company chooses to share that data, energy industry researchers and analysts can use it to create economic models and projections about future energy consumption. Again, this has been routine, time-honored practice for years. Online businesses did not invent it; they merely made the data-gathering process less expensive and more robust. Yet lawmakers seem bent on singling out Web commerce for heavy-handed regulation.

Part 4

The Psychology of Internet Privacy

The collection and use of customer information, within and outside its original context is not new. Yet only now, with the emergence of Internet-based analytics, has an uproar erupted. Why now?

Part of the answer goes back to a statement made early in this paper, that the Internet has exponentially increased the amount of information available while reducing the cost of both its acquisition and the application of analytics.

The other part is psychological, but a very real change nonetheless. The Internet has proved to be a means of documenting a large amount of one's personal information that, in the past, may not have been strictly private or confidential, but just limited to a handful of close friends and relatives. By and large, most of this information is relatively trivial, but nonetheless, when this information can literally circle the world in a matter of hours, the effect can be quite disconcerting. Remember, this is very new—Facebook didn't exist until 2004 and did not truly become a cultural touchpoint until 2007. Still, attempting to create rules that try to restrict the use of extant information is bound to prove fruitless. There are too many variables to consider. Let's explore this.

Classifying "on-line privacy," as if it were something different from other notions of privacy, creates something of a false label. All the Internet does is make it easier to collect information that was once difficult and time-consuming to get. For example, the law requires you to publish the price you paid for your home. For years this was confined to back-page newspaper listings, usually in a Saturday edition. In the past, it took considerable time and effort to research home prices. Today, because of the Internet, that information can be found in seconds.

Yet there is a degree of "future shock" in being able to not only see a picture of your home on the Web, but also see its current value by simply passing a mouse pointer over the photo. Nonetheless, this is not private and personal data, but information that's been traditionally available on the public record. And since it is difficult to show actual harm from its disclosure, it is why public officials need to be careful about calling for special restrictions simply because the data are stored as electrons on a magnetic disk instead of ink and paper in a metal cabinet.

More accurately put, when people talk about the "right to privacy," what they really mean is the right to control the disclosure of personal information about oneself. To a certain degree, the U.S. Constitution and common law respect this idea. Legally, a defendant cannot be compelled to testify

against him or herself. The law also respects the right of confidentiality between spouses, doctors and patients, attorneys and clients, and priests and penitents.

The government also protects the right of non-disclosure in certain civil arrangements. With only a few exceptions, employers cannot ask prospective employees about age, health history, marital status, religion or ethnicity.

Privacy, therefore, is foremost about boundaries. Philosophically, one can say the right to privacy derives from the human ability "to keep one's counsel." That is, one's thoughts are one's own and one has a choice whether or not to voice them. The law and civil society respect this choice by recognizing there are boundaries to the collection of personal information that cannot be forcibly crossed.

But boundaries are not solid walls; they imply a means of controlled access—a gateway through which certain parties can enter and others are refused. The implications the Internet has for information disclosure—that is, the adjustments it forces individuals to make in managing their privacy boundaries—is what's really sparked the controversy over information-gathering and tracking, and, in the end, who "owns" personal information and what rights they have to use it.

There are three categories of personal information, each with certain characteristics that have an impact on its disclosure and use.

- Undocumented information
- Documented information
- Deduced information

Undocumented information is knowledge you have about yourself that no others can know unless you personally disclose it. These pertain to unvoiced thoughts, but they can include sexual orientation, religious and political beliefs, or a high school crush. When shared, such information can be contained among a small group of people but otherwise remain undocumented or unconfirmed. Since undocumented personal information is often shared in confidence, there are ethical considerations that enjoin its wider disclosure, but disclosure is not necessarily illegal.

Documented information is information that you may or may not have widely disclosed, but is available to a third party through observation or research of the public record. This includes your address, your date of birth and your maiden name, but also extends to the value of your home, your previous addresses, your employers and other details. It is difficult for an individual to claim ownership of this information or a pre-emptive right to prevent its disclosure.

Inherent in this is that once information is documented, it is a verifiable fact that can be referenced. A husband may not want his wife to know that he spent a weekend in Las Vegas, but if the wife discovers his hotel bill from Caesar's Palace, the hotel did not violate his privacy.

Documented information is not assumed to be confidential unless there are specific laws, mandates or agreements against disclosure. Examples include adoption records, juvenile criminal records, court settlements and some contracts. Even those are not always absolute.

Here, the Internet's major paradigm shift is the way it documents information that most individuals could once assume would forever remain undocumented. Social networking provides the major dynamic, of course, but Web and search tracking also play a role.

> *There are two principal effects of the Internet on privacy. The first is to shrink personal expression to a dichotomy: public or private. Prior to the rise of digital social life, much of what we said and did was in a public environment—on the street, in a park, at a party—but was not actually public, in the sense of being widely broadcast or persistently available.*
>
> *This enormous swath of personal life, as we used to call it, existed on a spectrum between public and private, and the sheer inconvenience of collecting and collating theoretically observable but practically unobserved actions was enough to keep those actions out of the public sphere.*
>
> *That spectrum has now collapsed—data is either public or private, and the idea of personal utterances being observable but unobserved is becoming as quaint as an ice cream social.*[13]

This is a reality of the networked world. Regulations like Do Not Track and the White House Privacy Bill of Rights want to wish this reality away with legislation and regulation. But the proverbial genie can't go back in the bottle. When taken to its logical conclusion, we arrive at patently absurd proposals as the European Union's "Right to be Forgotten" Law.

Known colloquially as the "Internet eraser button," the EU, in the interest of preserving privacy, has proposed that citizens of member countries be given the opportunity to demand any website (European or not) expunge any information about them, even if it's true and documented by a third party. The EU proposal piggybacks on other efforts in Europe. According to the *Washington Post*, Spain's Data Protection Agency tried to force Google to remove links to material related to about 90 people. These included plastic surgeon Hugo Guidotti, who found that when his name was searched, Google's results returned a 1991 *El Pais* article about a $7.2 million lawsuit on breast surgery that allegedly went bad.[14]

The problem is that the information is part of the historical record and, whether the individual likes it or not (or in Guidotti's example, wins his case), it cannot be dispatched down a memory hole in the name of protecting privacy "rights." If the individual was dishonorably discharged from the military, that is a fact that cannot be erased. If an individual was convicted of a crime in a public court, that cannot be considered a private matter.

The Internet's other psychological paradigm shift involves deduced information. In terms of privacy protection, deduced information is the trickiest category because it attempts to extract undocumented information through collection and analysis of observations, patterns of behavior and documented information. A poker game offers a good example of the use of deduced information. In Texas Hold 'Em, you, as a player, are the only one at the table who knows exactly which two cards you hold. However, a good opponent, having paid attention to the way you've played previous hands, noted your past betting patterns and picked up subtle "tells" you may telegraph through body language and voice inflection, may be able to accurately deduce your hand.

On the other hand, deduced information is, at heart, a probability exercise. Its accuracy depends on the validity of the data inputs, the strength of the analytics and the skill of the analyst.

Just like in poker, often deduced information can never be confirmed and sometimes it can be wrong. That's why it's difficult to classify as a violation or intrusion.

However, as both market research techniques and the quality of information become better, deduced information can turn out to be extremely accurate. This indeed can spook consumers. The benefit of a free market, however, is that even as marketers experiment, they can pull back if they sense customer discomfort.

Big box retailer Target learned as much when it began an extensive research program to use buying patterns that would identify women customers who were pregnant. Prior market research showed that giving birth, as major life event, marks one of the few times that a customer's loyalty can change. The challenge for Target is that, like many other stores, it relied on tracking the types of purchases women made *after* giving birth—diapers, baby food, pacifiers, crib toys and such, primarily using data from loyalty cards. But by then, the opportunity to induce a change in loyalty had passed. So Target set out to attempt to statistically correlate the types of purchases women made three to six months into their pregnancy, and aggressively target them with mailers, coupons and other offers.

The subject was sensitive enough that Target closed off access to a *New York Times* reporter who, rather innocuously, had begun researching an article about how one of Target's employees used mathematical models to predict consumer behavior. While the company did not disclose the details about how it uses customer information to target consumers, it did admit that its profiling was accurate enough that some women were put off by a sudden deluge of pregnancy and infant-related product promotions, especially when the women themselves had kept the fact of their pregnancy known to just a few relatives. Target soon learned not to be too obvious about it, and in later mailers included coupons for other everyday items such as lawnmowers and wineglasses alongside coupons for diapers and cribs.[15]

This anecdote encapsulates several of the difficulties of regulating the use of information by online and Web-based enterprises. First of all, it shows that the practice of targeting advertising is not unique to the online world. In every industry, businesses look to use all the information they can

gather. Second, it shows that different types of documented information can be combined to create information that is both strategic and proprietary—in the Target case, a profile strong enough to identify a pregnant women with a profitable degree of accuracy. Third, none of this breaks any current laws, nor compromises security, nor violates any ethical norms.

Has the pregnant woman's privacy been violated? At the risk of invoking an academic argument, it's fair to answer no. Target does not know for certain whether the pregnancy is a fact. It only has statistical evidence that points toward it. Likewise, online, behavioral ads are served on the basis of statistical probability.

For different reasons, industry and regulators need to keep these new paradigms in mind. The industry needs to respect consumer pushback on information collection. Companies like Google and Facebook can move—and at times have moved—too fast for their users. Lawmakers, however, need to be careful about interpreting user complaints as a call for massive regulatory control. Users want to feel secure about controlling the disclosure of their information; but they don't want to be barred from doing so.

Lawmakers and regulators also need to be aware there is no malicious intent behind this type of information-gathering. What the website is trying to do, and help its advertisers do, is establish and strengthen a commercial relationship with the customer. Lawmaker misunderstanding is explicit in the very name given to "Do Not Track" bills. Websites and advertisers do not actually "track" individuals like stalkers as they surf the Web. What sellers try to do is create a statistical profile of a likely customer and then look for individuals who fit it. This profiling is done by computers, not people, which are aggregating data from millions of inputs. It's not personal.

> *Being observed by an insect on the wall is not invasive for privacy; rather, privacy is threatened by being subject to human observation, which involves judgments that can affect one's life and reputation. Since marketers generally are interested in aggregate data, they do not care about snooping into particular people's private lives. Much personal information is amassed and processed by computers; we are being watched not by other humans, but by machines, which gather information, compute profiles, and generate lists for mailing, emailing, or calling. This impersonality makes the surveillance less invasive.*
>
> *While having one's actions monitored by computers does not involve immediate perception by a human consciousness, it still exposes people to the possibility of future review and disclosure. In the context of databases, however, this possibility is remote. Even when such data is used for marketing, marketers merely want to make a profit, not uproot a life or soil a reputation.*[16]

Part 5

The Dangers of Misapplied Privacy Regulation

The European experience with its Privacy Directive provides a sobering illustration of the effects of regulations designed to curtail online targeted advertising and the information-gathering and processing mechanisms that make it possible.

The experience is significant because the White House "Online Privacy Bill of Rights" closely follows the latest revision of the EU Directive, including the right to "context," that is, personal data cannot be used for any other reason other than for what it was collected. The latest EU draft calls for fines as high as €1 million, or up to 2% of a company's global annual revenues, for violations.[17]

The EU Privacy Directive dates back to 1995, although it did not become effective across all member countries until 2004. The directive is binding on any company doing business in Europe and can be highly restrictive. For example, the EU is currently claiming that Google's new privacy policy, in which they will combine user information across some 60 of its service platforms, violates the Directive.

Generally, however, the information-gathering and processing must be done by companies doing business in the EU. U.S.-based websites with no European presence are not subject to the directive, even though users in the EU countries may visit them.

Since the Privacy Directive was going into wide effect just as search engines were perfecting targeted ad platforms and social media was taking off, it offers a side-by-side comparison with the U.S. of how, over the past eight years, its regulations slowed the growth of Web media in Europe.

An analysis of the Web advertising market undertaken by researchers at the University of Toronto found that after the Privacy Directive was passed, online advertising effectiveness decreased on average by around 65% in Europe relative to the rest of the world.[18]

Even when the researchers controlled for possible differences in ad responsiveness and between Europeans and Americans, this disparity manifested itself.

> *We found that when Europeans browsed websites outside of Europe (mostly in the U.S.) that were not affected by these laws, there was no reduction in ad effectiveness. Conversely, when non-Europeans browsed EU websites that were covered by the laws, there was a reduction in ad effectiveness. This suggests that the change in effectiveness we observe is not linked to time-varying changes in consumer attitudes in Europe relative to the U.S.*[19]

The authors go on to conclude that these findings will have a "striking impact" on the $8 billion spent each year on digital advertising: namely that European sites will see far less ad revenue than counterparts outside Europe.

Furthermore, the authors found that general interest sites fare far less well in the EU than websites that have specific content. As noted earlier, just by visiting a specialized website, a user discloses information about herself, so there is a built-in targeting effect. Meanwhile, the success of general interest sites, such as news and media services, which in the U.S. rely heavily on targeted advertising, is hindered significantly by the EU rules.

> *Websites that had general content unrelated to specific product categories (such as news and media services) experienced larger decreases in ad effectiveness after the laws passed than websites that had more specific content (such as travel or parenting websites). Customers at travel and parenting websites have already identified themselves as being in a particular target market, so it is less important for those websites to use data on previous browsing behavior to target their ads. The Privacy Directive also disproportionately affected ads that did not have additional visual or interactive features. One interpretation is that plain banner ads' effectiveness depends on their ability to be appropriate and interesting to their audience. Therefore, the laws curtailing the use of past browsing behavior to identify a target audience for the ads would affect plain banner ads disproportionately. We also find that the Privacy Directive affected ads that had a small footprint on a webpage more than those with a large footprint.*
>
> *Furthermore, we show that the loss in effectiveness has been particularly pronounced for websites with more general content that could not be easily linked with a specific product, such as news and web services sites. These websites have content that is already not easily monetizable. The privacy regulation makes monetizing it even more challenging. This suggests that stronger regulations may make it harder for ads running on general content websites to be effective, relative to ads running on websites that are linked to specific product categories. In addition, we found that privacy regulation is related to reduced effectiveness of ads that did not have interactive, audio, or visual features. Again speculatively, we suggest that as the use of customer data by marketers online becomes increasingly regulated, ads may become more obtrusive.*[20]

Although it is difficult to prove a negative, it is arguable at least, that the EU Privacy Directive handicapped the development of Web media in Europe. There are no European search engines that rival even smaller U.S.-based Web search companies. Unlike in the U.S., social networking in Europe comes at a fee. Hyves, a Netherlands-based competitor of Facebook, has tiered service. Basic access is free, but to take advantage of more common social networking features, such as

uploading photos and videos, users must purchase a "Gold Member" subscription. No EU-launched social network company has grown to a significant size, even though the entry of U.S.-based Pinterest and Foursquare demonstrates there is still room for growth, innovation and investment in the sector.

Meanwhile, European wireless manufacturers seem to be missing the wireless data revolution, which exploits the location-tracking ability smartphones have. Nokia, once the world leader in wireless handsets, has faded in the wake of Apple's iPhone and Google's Android mobile operating system. Both technologies allow applications to access user data, especially location information, to provide users with massive utility. GasBuddy, an app that lists gasoline prices at nearby service stations is one of the best of the latest examples. True, Nokia had problems developing a competitive operating system, but how many of those problems can be traced to the Privacy Directive's regulations, which pre-empt information-sharing across application platforms without explicit user permission?

But speculation aside, the most telling fact about EU regulation is that two major innovators in Web media platforms—Google and Facebook—face investigation and penalties from European regulators over privacy. In this regulatory environment, what European entrepreneur or venture capitalist is going to risk investing in a start-up in Web media? And more importantly, why would U.S. lawmakers ever see wisdom in importing this model?

Part 6

Other Unintended Consequences

A. Free Services Go Away.

As noted, hundreds of thousands, if not millions, of sites support themselves through targeted advertising. If the federal government began to clamp down on websites' ability to use consumer information to target ads, an immediate consequence would be a decline in the amount of free content, information and services available on the Web. If we consider the usage data from Europe, it is likely the general interest sites, those dealing with news, reference, how-to and entertainment that runs a gamut of tastes will have the toughest challenge in this type of regulatory environment. Ironically, many of these sites are offshoots from the reputable newspapers and magazines a number of legislators have said they want to preserve. Yet, instead of creating a cumbersome subsidy system, which has been proposed in Congress and by the FCC, the viability of established media might be maintained by simply allowing Web business models to work.

The same goes for entrepreneurs seeking to set up Web-based services from scratch. From a software standpoint, many of the tools that a start-up site requires are available off-the-shelf at low cost, or no cost at all, such as Google AdSense. Regulation would add a new compliance burden on any start-up hoping to use targeted ads, creating an obstacle that would affect capitalization requirements at best and kill the business model for free services at worst. Hyves, the Dutch social network which charges for users for access to many features, demonstrates this.

B. "Mother May I?" Trumps Experimentation.

Regulation forces companies to evaluate compliance issues before pursuing a potentially innovative product or service direction. As a result, innovation is slowed, or does not happen at all, not because of market considerations, but on the advice of legal counsel. This is a major risk of any regulation or legislation in technology, an area that is constantly changing and evolving, and where success and survival often hinge on out-of-the-box thinking. It is another reason why guidelines are preferable to law.

Moves such as Google's new privacy policy, which brings together user information from some 60 of its separate services into a single database, may generate controversy, but they also help

determine market boundaries. In any young technology or service, controversy and debate should be welcome.

Google is testing the privacy paradox. There indeed may be enough significant user backlash that Google backs off. This has happened several times with both Google and Facebook, and both nonetheless remain popular and well-regarded. With this mind, lawmakers will serve consumers best if they allow companies to experiment with the privacy paradox to find where actual boundaries are, rather than hamstringing potential innovation by pre-emptively and blindly setting them.

C. Regulations Against Information-Sharing Undermine the Community-Building Benefit of the Medium.

One of the reasons people go online is to meet and interact others who share interests and passions. Individuals with unique interests—from birdwatching to numismatics to Axis & Allies gaming—can connect with far more like-minded individuals than they might in their own geographic community. These communities in turn build knowledge bases that the general population of users can turn to from time to time. For example, someone planning a vacation in New York City can use Google to find a bevy of bulletin boards and forums, some quite granular, that provide information about shows, restaurants and attractions, all from people who have shared their experience. These boards thrive because search engines like Google and social networks like Facebook drive traffic to them—all based on preferences. Regulate this technology away and the Web loses its unique community-building and "crowd-sourcing" character.

D. Proposed Privacy Rights Won't Address Information Security.

Politicians often conflate privacy and security. The two are related, but are not the same thing. Security pertains to the protection of critical user information that, if disclosed, can result in theft or fraud. Neither Do Not Track nor the on-line privacy "bill of rights" truly addresses security issues related to on-line information.

Wire fraud laws already make it illegal to steal user information. Identity theft and identity fraud are crimes. Companies that fail to adequately protect confidential and sensitive information suffer legal consequence. For example, retailer T.J. Maxx was required to pay $9.75 million as part of settlement with 41 state attorneys general after thieves obtained credit card information from thousands of T.J. Maxx customers because a store was transmitting them on an unsecured wireless link. Belmont Savings Bank in Massachusetts was fined $7,500 after the bank lost an unencrypted backup computer tape containing personal information of more than 13,000 customers.

By contrast, the information websites collect, collate and process for targeted marketing is not highly personal and confidential, such as social security numbers, banking information or specific health-related data, that in the wrong hands could be used for malicious purposes.

On the contrary, most of the information search engines, social networks and e-commerce sites glean has to do with individual habits and preferences that could otherwise be easily observed—does the person prefer beer or wine? The Cubs or the White Sox? Mystery novels or biographies? Michael Bay or Mike Leigh? For the most part, it is anonymized. True, Facebook and other sites allow users to post pictures and disclose more intimate personal details such as religion or sexual orientation, but again, *users can decide* whether to disclose these facts and, if they do, decide who may see them. Opt-in, Do Not Track and privacy bills of rights are all about substituting government mandates for individual discretion. They do not strengthen or expand on any current laws against online fraud or theft, which by themselves are quite strong.

Part 7

How the Market Effectively Addresses Privacy Issues

Another reason to go slow on privacy regulation is that the market has shown a remarkable ability to correct itself much faster than government action. This is all the more critical because of the way users balance privacy against the benefits of disclosure.

We have briefly touched on the "privacy paradox" at different points so far, but lawmakers must understand it as a significant factor in consumer website interaction before creating a regulatory environment that consumers don't really want.

The term "privacy paradox" has been around for almost ten years. Boiled down, it describes the repeated finding that while individuals express a high degree of concern for privacy protection online, few, in practice, take advantage of privacy safeguards when they are offered.

This apparent contradictory behavior has been noted in a number of studies, including a noted 2007 paper in the *Journal of Consumer Affairs*.[21] Separately, a 2005 Pew Internet Study, cited by Forbes, found that that 54% believe that websites invade their privacy when they track behavior. But the same study showed that 64% were willing to give up personal information to get access to a website.

In the marketplace, when search engines like Google began facing vocal pushback from users and regulators on its tracking of user search histories, one of Google's competitors, Ask.com, tried to differentiate itself by unveiling AskEraser. Just like it sounds, the tool allows users to opt out of search tracking, just the sort of tool Do Not Track legislation would force on users. But as Forbes reported at the time, despite their apparent clamor for the opt-out tool, users didn't switch from Google to Ask in order to use it. AskEraser did nothing for Ask's market share, while Google's continued to grow.[22]

Pinterest serves at the latest example of the privacy paradox in action. Although surveys do show consumers concerned about their privacy and their information disclosure on the Web, Pinterest is taking off precisely because it allows users to share much more, not less.

"With Facebook, a lot of the status updates are things you really don't care about," one consumer told a *Houston Chronicle* reporter. "With Pinterest, you can actually target the things that you like. I love it so much. I'm on all the time."[23]

The Chronicle cited a comScore metric finding that Pinterest drew 11.7 million unique monthly visitors in January 2012, making it the third-fastest-growing site since December 2011. According to content sharing firm Shareaholic, Pinterest drove 3.6% of all Web traffic referrals to other sites in January, more than Google+, LinkedIn and YouTube combined. Pinterest placed just behind Twitter for fourth place on that traffic referral list, with Facebook No. 1 at 26.4%.

And since Pinterest became one of the apps that plug into Facebook's Timeline member profiles last month, the number of Facebook users visiting the site every day has jumped by 60%.[24]

> *While Facebook has found monumental success as a general social network based on building a network of friends, Pinterest, based in Palo Alto, Calif., has carved a niche as a social network based on finding and sharing topics that users are passionate about.*[25]

There is a temptation by some, including consumer protection groups like Consumers Union, to argue that the privacy paradox is the result of user ignorance about their browser features or the privacy settings on various websites. Hence, they invoke a paternalistic rationale for regulation—that the government needs to "protect" people from their own lack of knowledge or lack of judgment.

The problem is that privacy is subjective. The willingness to share personal information differs from person to person. To be sure, some people might be injudicious online and embarrass themselves, but people have been embarrassing themselves long before the Internet appeared on the scene. Unless their behavior posed harm to others, the government saw no need to step in.

Since privacy is subjective, it is impossible to design an acceptable government mandate that would limit the ability of websites to acquire and share certain kinds of information. Some people will almost certainly feel that too much information is being disclosed regardless of the "strength" of any such mandate, while others will object that they are not able to benefit from the tailored offerings that are made possible by the use of information acquired as a result of their browsing habits.

In the end, the best policy is to allow individuals to match their online sharing with their comfort level. The privacy paradox itself is becoming more complex over time as browser software, as well as search and social networking sites, have evolved their privacy settings to give users more and more choice. In direct contradiction of the paternalistic argument, research shows that users have started taking responsibility for their own privacy, learning about and exercising options in line with their own preferences, not those of a privacy nanny.

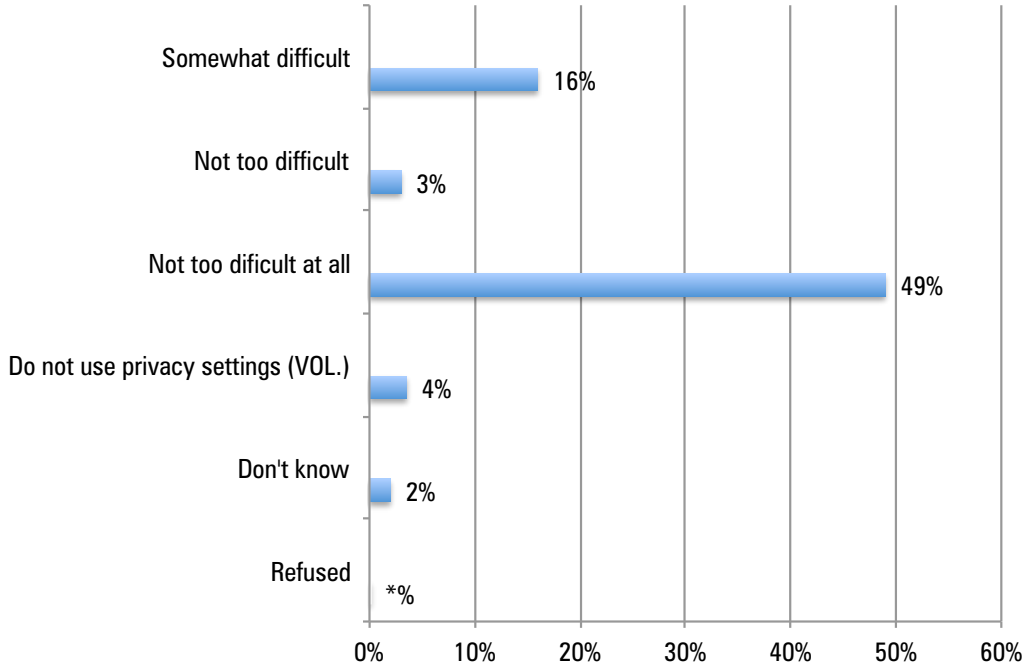
A 2009 study of the privacy paradox reviewed findings of a number of surveys of social networking done between 2005 and 2008. All found that only a small percentage changed the

default privacy settings. One 2007 study analyzed more than 20,000 MySpace profiles and found that only 27% were set to private. Another 2008 study downloaded the Facebook profiles of a whole class of a private American university and found that only one-third was set to private. Yet another 2007 study found a similar percentage among on Hyves users.[26]

A new study, published in February 2012 from the Pew Research Center's Internet & American Life Project shows how much this has changed. The survey found that a majority of social network site users (58%) restrict access to their profiles. Women are significantly more likely to choose private settings—only 20% said their main profile is set to be completely public. Women who use social networking sites are more likely than men to set the highest restrictions (67% vs. 48%).[27]

While half of social networking site users say they have some difficulty in managing privacy controls, just 2% said it is "very difficult" to use the controls. The balance—49%—said setting privacy controls was "not difficult at all." Ironically, Pew found that those with the most education reported the most trouble with the controls.

Figure 1: Difficulty in Managing On-line Profiles

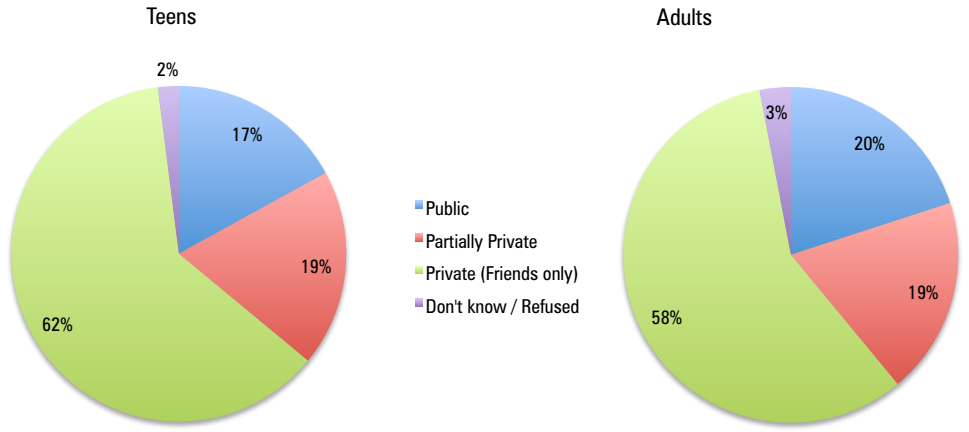


Source: The Pew Research Center's Internet & American Life Project, April 26–May 22, 2011 Spring Tracking Survey

The report also dispelled the common myth that younger people do not understand the consequences of disclosing personal information or are generally not as concerned with privacy as their elders. When looking at social media usage patterns, age tends to be one of the strongest variables. For instance, younger users have long been the most active users of the sites and the

most active managers of their online reputations. However, when it comes to basic privacy settings, users of all ages are equally likely to choose a private, semi-private or public setting for their profile. There are no significant variations across age groups.[28] Private settings also have become the norm, Pew found, regardless of age.

Figure 2: Teens' and Adults' Privacy Settings on Social Media Sites



Source: The Pew Research Center's Internet & American Life Project, April 26–May 22, 2011 Spring Tracking Survey

> *The choices that adults make regarding their privacy settings are virtually identical to those of teenage social media users. Close to two-thirds (62%) of teens who have a social media profile said the profile they use most often is set to be private so that only their friends can see the content they post. One in five (19%) say their profile is partially private so that friends of friends or their networks can see some version of their profile. Just 17% say their profile is set to public so that everyone can see it. This distribution is consistent regardless of how often a teen uses social network sites.*[29]

More users also are tending their profiles, keeping their information up-to-date and deleting unwanted friends, comments and photo tags. Almost two-thirds of profile owners (63%) have deleted people from their networks or friend lists, up from 56% in 2009. Another 44% said they have deleted comments that others have made on their profile, up from just 36% two years prior. And as photo tagging has become more automated on sites like Facebook, users have become more likely to remove their names from photos that were tagged to identify them; 37% of profile owners have done this, up from 30% in 2009.[30]

This behavior refutes assertions by would-be regulators, such as Sen. Charles Schumer, a vocal supporter of social media regulation. In a 2010 letter the FTC, Schumer wrote that Facebook's privacy policies "have limited the ability of users to control the information they share and keep private."[31]

Part 8

Conclusions

Examination of the technology, business models, and consumer research supports a light-touch approach to the regulation of websites with regard to the use of personal information. Technology moves too quickly for legislation to keep up. Entrepreneurs need to have freedom to explore new business models without looking over their shoulder for fear of a government crackdown. Finally, consumers show a willingness to exchange information about their tastes and lifestyles in return for the tangible value of free services.

The case for allowing free market models to shape the way consumers chose to interact with websites can be summarized in five points.

A. Top-Down Mandates Slow Technology Innovation.

Legislative and regulatory directives pre-empt experimentation. Consumer needs are best addressed when best practices are allowed to bubble up through trial-and-error. When the economic and functional development of European Web media, which labors under the sweeping top-down EU Privacy Directive, is contrasted with the dynamism of the U.S. Web media sector, which has been relatively free of privacy regulation, the difference is profound. U.S. Web entrepreneurs continue to push the envelope in terms of creativity and innovation. Facebook, LinkedIn, Groupon, Foursquare and Pinterest are just a handful of popular sites that have emerged since 2004, just as the EU Policy Directive was taking effect across the continent. It is telling that no analogs to these ventures have arisen in Europe. Additional research shows that overall, the effectiveness of Web-based advertising is far lower for sites in Europe, where targeted advertising is regulated, than it is in the U.S.

B. Consumers Push Back when They Perceive that Their Privacy Is Being Violated.

Google and Facebook, two of the largest and most visible Web-based enterprises that collect user data, have felt user backlash on several occasions when they have changed their privacy policies or, in the eyes of users, disregarded them. In every case, the company reacted far more quickly than the government could. When the FTC did finally render judgment, it could find no harms worthy of fines or sanctions. Just as important, despite their missteps, neither Facebook nor Google lost much in terms of user goodwill. Their CEOs apologized and promised to do a better job

communicating privacy policy and any changes. They serve as excellent examples of how the market can correct itself when consumers express displeasure.

C. Web Advertising Lives or Dies by the Willingness of Consumers to Participate.

As a corollary to the point above, websites that derive revenues from targeted advertising must be sensitive to user perception because if users believe they have been exploited, they will stop visiting the site. Although Google and Facebook are dominant at the moment, there are no guarantees that they will remain so. MySpace is an example of a social network that dominated its sector. But its reputation as being a largely unsupervised community for teens, its susceptibility to phishing, malware and spam, as well as (overblown) reports of its being an easy source of pornography and a haven for child predators ultimately proved fatal. In early 2008, MySpace was still the most visited website in the world. One Web metrics firm, comScore, estimated that MySpace traffic had dropped to 63 million unique users from 95 million in the 12 months between February 2010 and 2011.[32] As of March 2012, MySpace ranked 160th on Alexa, another Web metrics site.[33]

Facebook and LinkedIn, however, learned from MySpace's mistakes, which, to be fair, were largely due to its being the first major social networking player. Nonetheless, MySpace's failures to adequately meet user satisfaction levels, especially after Facebook and LinkedIn arrived on the scene, demonstrates that users will move away from a popular site if they are unhappy with its privacy approaches.

D. Allows Customers to Customize Their Unique Privacy Wishes.

Privacy concerns are best addressed through clear policies and contractual agreement. Well-crafted legislation can endorse this, yet still leave room for users to set their own privacy parameters in line with their own preferences.

Privacy policies can be enforced via the FTC or the courts, the latter being preferable. This process has worked well in the area of information security, and courts have found retailers such as T.J. Maxx and banks such as Belmont Savings Bank in Massachusetts liable for consumer loss because of data breaches.

E. Greater Information Availability Is a Social Good.

An unfortunate aspect of the call for privacy regulation is the *a priori* assumption that commercial information-gathering and targeted advertising are questionable practices from which consumers need to be protected. In fact, information-gathering has a long history in all areas of market research—especially audience research in media. It is also clear from the evidence that consumers

are willing to provide information about age, gender, income, lifestyle, preferences and tastes in return for more streamlined and customized information about products and services which might interest them, as long as they are satisfied that the information they provide will be confidential or anonymized.

While these mechanisms serve the specific needs of buyer and seller, it is worth noting that there are wider social benefits when more information is available to buyers and sellers. For one, limited resources can be allocated better. Suppliers can know which regions of the country will have the greatest demand and adjust their distribution networks to meet it. Product goes to where it's most needed; better value is derived from transportation costs, and there is less waste. These are just basic examples. Multiplied across global markets and applied to hundreds, if not thousands, of information parameters and variables—all processed at very low cost—productivity and wealth begins to grow throughout the economic ecosystem.

Nothing is more counterproductive to an information economy than government policies designed to deliberately inhibit the voluntary exchange and use of information. Right now, search, social media and informational websites are the most visible users of consumer information, but in the background, many of the automated, intelligent services we expect the Web to support will need to trade in user information. These include such basic applications as Web-enabled home appliances, such as refrigerators that sense when you're low on milk to more critical services such as health care management. This is why it's best to derive privacy policies from a strong and constantly evolving knowledge base of best practices, rather than to codify them into laws that, in their failure to foresee innovation, will discourage it.

Endnotes

1 Shane Richmond, "Pinterest: The New Hit Social Network Explained," *The Daily Telegraph*, Feb. 28, 2012, available at http://www.telegraph.co.uk/technology/social-media/9111278/Pinterest-the-new-hit-social-network-explained.html

2 Mary Madden, "Privacy management on Social Media Sites," Pew Research Center's Internet & American Life Project, Feb. 24, 2012, pp. 6-8, available at http://pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx

3 Statistics summary for myspace.com, http://www.alexa.com/siteinfo/myspace.com, Accessed March 21, 2012. This data updates daily, but the metric generally hovers between 120 and 180.

4 Richmond, "Pinterest."

5 Avi Goldfarb and Catherine E. Tucker,"Privacy Regulation and Online Advertising," University of Toronto, August 5, 2010, p. 7, available at http://ssrn.com/abstract=1600259

6 Vangie Beal, "What are Cookies and What Do Cookies Do?" Webopedia, posted: Sept. 4, 2008, last updated: Aug. 31, 2010, available at http://www.webopedia.com/DidYouKnow/Internet/2007/all_about_cookies.asp

7 Goldfarb and Tucker, "Privacy Regulation and Online Advertising," p. 9.

8 Jefferson Graham, "YouTube Keeps Video Makers Rolling in Dough," *USA Today*, Dec. 16, 2009, available at http://www.usatoday.com/money/media/2009-12-16-youtube16_CV_N.htm

9 "Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises," Nov. 29, 2011, U.S. Federal Trade Commission Website, http://ftc.gov/opa/2011/11/privacysettlement.shtm.

10 Ibid.

11 Mark Zuckerberg, "Our Commitment to the Facebook Community," The Facebook Blog, Nov. 29, 2011, available at https://blog.facebook.com/blog.php?post=10150378701937131.

12 "FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network," March 30, 2011, U.S. Federal Trade Commission Website, http://www.ftc.gov/opa/2011/03/google.shtm

13 Clay Shirky, "What 'Public' Means Now," part of "Room for Debate: Should Government Take On Facebook?," *New York Times*, May 25, 2010, available at http://roomfordebate.blogs.nytimes.com/2010/05/25/should-government-take-on-facebook/

14 Elizabeth Flock, "Should We Have a Right to Be Forgotten Online?" Washington Post BlogPost, April 20, 2011, available at http://www.washingtonpost.com/blogs/blogpost/post/should-we-have-a-right-to-be-forgotten-online/2011/04/20/AF2iOPCE_blog.html

[15] Charles Duhigg, "How Companies Learn Your Secrets," *New York Times Magazine*, Feb. 18, 2012, available at http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

[16] Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy," *Stanford Law Review*, Vol. 53, p. 1393, July 2001, Available at http://ssrn.com/abstract=248300

[17] Kelly Fiveash, "EU commissioner unleashes draft data protection bill," *The Register*, Jan. 25, 2012, available at http://www.theregister.co.uk/2012/01/25/viviane_reding_data_protection_draft_bill/

[18] Goldfarb and Tucker, "Privacy Regulation and Online Advertising," p. 4.

[19] Ibid.

[20] Ibid, pp. 4-5, 31-32.

[21] Patricia A. Norberg, Daniel R. Horne, and David A. Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs*, vol. 41, no. 1 (Summer 2007), pp. 100–126.

[22] Andy Greenburg, "The Privacy Paradox," Forbes.com, Feb. 8, 2008, available at http://www.forbes.com/2008/02/15/search-privacy-ask-tech-security-cx_ag_0215search.html

[23] Benny Evangelista, "Pinterest Pins Down Followers," *Houston Chronicle*, Feb. 29, 2012, p. D1, available at http://www.chron.com/business/article/Pinterest-pins-down-followers-3368760.php

[24] Ibid.

[25] Ibid.

[26] Sonja Utz and Nicole C. Krämer, "The Privacy Paradox on Social Network Sites Revisited: The role of Individual Characteristics and Group Norms," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 3 (2), article 1, 2009, available at http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1

[27] Madden, "Privacy management on Social Media Sites," pp. 6–8.

[28] Ibid, p. 6.

[29] Ibid, p. 7.

[30] Ibid, p. 9.

[31] Cristian Salazar, "Senator Schumer Asks FTC To REGULATE Facebook, Social Networks," Huffington Post, April 26, 2010, available at http://www.huffingtonpost.com/2010/04/26/ftc-facebook-regulation-s_n_551910.html

[32] Emma Barnett, "MySpace Loses 10 Million Users a Month," *Daily Telegraph*, March 22, 2011, available at http://www.telegraph.co.uk/technology/myspace/8404510/MySpace-loses-10-million-users-in-a-month.html

[33] Statistics summary for myspace.com, http://www.alexa.com/siteinfo/myspace.com, Accessed March 21, 2012. This data updates daily, but the metric generally hovers between 120 and 180.

Reason

Reason Foundation
5737 Mesmer Ave.
Los Angeles, CA 90230
310/391-2245
310/391-4395 (fax)
www.reason.org