Before the
Federal Trade Commission
Bureau of Consumer Protection

"Reboot Online Privacy"

Comments of
Reputation.com, Inc.

regarding
the Preliminary FTC Staff Report entitled

"Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

File No. P095416

February 18, 2011

Michael Fertik
Chief Executive Officer
Reputation.com, Inc.
2688 Middlefield Road, Bldg C
Redwood City, CA 94064
(877) 720-6488

Comments of Reputation.com, Inc.

Reputation.com, Inc. respectfully submits these comments in response to the FTC's Preliminary Staff Report entitled "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." [1] By way of background, Reputation.com, Inc. (formerly known as ReputationDefender, Inc.) is a privately-held Silicon Valley company dedicated to helping consumers regain control over their online privacy and reputation. With tens of thousands of customers in more than 100 countries worldwide, Reputation.com is the world leader in empowering consumer privacy. Most recently, Reputation.com, Inc. was named a World Economic Forum ("Davos") Technology Pioneer for 2011.[2]

Introduction: Consumers need a full privacy reboot

The Federal Trade Commission's investigation of consumer privacy could not come at a more important time: Online consumers feel powerless against privacy threats from countless sources. They often don't understand how their data is being collected and used, nor what they can do to stop it. Consumers have expressed concern about threats ranging from behavioral advertising that seems to track their every movement, through "white pages" sites that give away their home address, to unsolicited email, to private information posted on social networking sites. Consumers have vociferously objected to different practices at different times, but no single vision has emerged for the right way to unify consumers' privacy expectations and experiences across a range of privacy concerns. Various incremental solutions have been proposed to address different parts of the online privacy ecosystem: ranging from voluntary do-not-track browser headers, to cookie-blocking browser add-ons, to a "do not email" registry, to browser plug-ins that generate fake behavioral data. Each of these methods can improve privacy if used properly, but these individual innovations resemble a game of Whac-a-Mole® as new privacy threats emerge faster than solutions can be created.

Some commentators have suggested that the government develop specific regulations for each industry, data source, or data use as it emerges. While this method will be effective for certain high-priority privacy threats, it cannot solve all threats to consumer privacy. An overall industry-by-industry or source-by-source strategy to develop detailed regulations will be stymied by technological change that renders classifications and regulations moot almost as soon as they are created. In

[1] Reputation.com respectfully makes additional reference to its response to the Department of Commerce's notice of inqury concerning online privacy. The company's response may be found at: http://www.reputation.com/blog/2011/01/31/reputation-com-comments-commerce-department-privacy-green-paper/

[2] See release and accompanying information at http://www.reputation.com/press_room/reputationdefender-honored-as-world-economic-forum-technology-pioneer-2011/

addition, every consumer has unique preferences as to how his or her data is used: some might publicly broadcast their most personal secrets through Facebook or a blog, while others might seek customized content and web pages based on their behavioral profile, while yet others might prefer that no information about them be publicized, analyzed, stored, or used at all.

Instead of reliance only on incremental regulations, it is time for a full reboot of consumer privacy. Through careful regulation and powerful enforcement, a pro-privacy economy can be create that will give consumers power to control how their data is used, to monitor for compliance, and to revoke access to that data when it is no longer needed. Government regulation and enforcement will create the conditions for consumers to exercise their own empowerment, according to their own privacy preferences. Solutions like "Do Not Track" that address high-priority privacy threats can be an important foundation of the pro-privacy economy, but they are not the end of the story. Instead, core foundational rules can create leverage for consumers and advocates to enforce their own preferences, and to update those preferences as technology and privacy threats change.

These foundational rules should bring a fresh perspective to consumer privacy, starting from first principles rather than simply accepting the current status quo. There is no reason to believe that current privacy defaults are ideal for consumers; in fact, there is ample reason to believe they are not. It is not enough to accept that large Internet companies have been treating their privacy practices as a matter of *fait accompli* and then suggesting that the market supports those practices simply because they have been grudgingly tolerated. Instead, we have the opportunity to create new default rules that will better balance the interests of consumers, businesses, advertisers, and communities.

A properly-regulated privacy economy will support online business innovation. By setting and enforcing core baseline rules, new privacy-protective business models will emerge, and innovative companies will be able to make better and more secure use of data. True innovation will expand beyond online advertising; instead, new companies will invent innovative and productive uses of data that consumers have entrusted to them, empowered by their confidence in the baseline rules. It is impossible to predict the exact businesses that will emerge, but they can range from consumers choosing to share medical data with a trusted group, to sites that gain consumer consent to gather useful statistics about their habits, to businesses which offer a more personalized experience and content to consenting consumers. These new and valuable services can only be produced if consumers feel confident in sharing their data, if businesses understand the rules under which they can use it, and if regulation is flexible enough to accept changes in technology and innovative new business models.

Innovations like "Do Not Track" and privacy-by-design enhance privacy, but are not a comprehensive solution

Innovations like a "Do Not Track" system and clear "privacy by design" guidelines can make it easier for consumers to express their privacy preferences in some situations——especially when supported by flexible regulations and predictable enforcement. But the "Do Not Track" model addresses only data that is collected directly from tracking users' activities and not the other vast flows of data that a consumer may not even know exist. And the "privacy by design" model provides useful guidance for many companies, but does not address sites which intentionally or knowingly publicize information as part of their business model.

As the Commission and other observers have correctly noted, consumers are not adequately empowered by the current notice-and-consent model when dealing with behavioral advertising networks that may threaten their privacy. It is time-consuming for consumers to find and understand the privacy terms of tens or hundreds of sites per day: as just one example, Facebook's privacy policy is more than 5,500 words long, in addition to 3,900 words of general terms and conditions, 1,600 words of special terms for users who make purchases on the site, and more than 500 additional words of "Facebook Principles."[3] Consumers don't always realize all the implications of their actions, especially when advertising networks track them across sites or in unexpected ways. And it is difficult for consumers to express their privacy preferences to sites: not all sites allow opting out of certain features, and other sites require complex steps to express privacy preferences. Consumers are simply overwhelmed.

Technology combined with proper implementing regulations (such as the "Do Not Track" system) can reduce friction in these privacy relationships and make it easier for consumers to express their privacy preferences. A "Do Not Track" system is simply a way for consumers to communicate a tracking preference to all sites they visit. When combined with appropriate regulation and enforcement, consumers can trust that their preference will be respected, even if it means that they will not have access to certain website features. This automated communication is far more efficient than requiring consumers to find the privacy settings for each site, determine if the site allows opting-out of behavioral tracking, and locate a way to express that preference. And automated communication is crucial when one website may host advertisements from many different advertising companies: for example, the Wall Street Journal found that the site Dictionary.com used at least 168 different tracking tools, many from different advertising companies.[4]

---

[3] Facebook, "Facebook's Privacy Policy," December 22, 2010 (http://www.facebook.com/policy.php).

[4] Julia Angwin and Tom McGinty, "Sites Feed Personal Details to New Tracking Industry," THE WALL STREET JOURNAL, July 30, 2010 (http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html).

Clear guidance and best practices for "privacy by design" can also assist companies in making responsible use of consumer data. For example, businesses should set privacy-protective default settings: recent experience shows that two-thirds of Facebook users have not customized their privacy settings, despite repeated changes to Facebook's privacy policies and the amount of data that the company made publicly available.[5] By promoting understanding that there is no privacy-neutral default setting and encouraging businesses to set privacy-promoting defaults, consumer privacy will be enhanced. Other privacy-by-design principles, ranging from data anonymization through automated deletion, can also present clear guidance to companies that want to do the right thing.

Other similar technological-regulatory solutions can also help empower consumers in other limited circumstances: there have been proposals for standard graphical privacy icons[6] or machine-readable privacy terms[7], that allow consumers to quickly understand how their personal-information will be used by a given site. In some ways, these information-communicating features are similar to the "Nutrition Facts" labels on food products that make it easy for grocery-store consumers to compare different brands; think of standardized graphics as "Privacy Facts" that consumers can use to compare privacy policies.

There are many privacy problems beyond "Do Not Track" and privacy-by-design principles

Behavioral ad tracking is not the only threat faced by consumers. In fact, behavioral ad tracking is only the visible tip of the privacy iceberg. Savvy consumers are increasingly discovering that information they consider to be private is being used, sold, and distributed online; often with no involvement from the consumer and against the consumer's wishes. To take just one prominent example, many "people search" or "white pages" websites allow any Internet user to look up any U.S. resident's home address, phone number, spouse's name, children's name, other household members, approximate income, approximate wealth, home value, and often even a photograph of their home from street level.

Many of these "people search" sites draw their information by assembling public records, such as voting records, marriage certificates, professional licenses, and real estate records. Others combine social networking information with marketing information gathered from offline sources,

[5] FTC Preliminary Report at 28, n.68.
[6] Such as Aza Raskin's description of "Privacy Icons" depicting standardized privacy policy terms in simple graphics. (http://www.azarask.in/blog/post/privacy-icons)
[7] See, for example, the W3C's previous attempt at creating a "Platform for Privacy Preferences" to create machine-readable standardized privacy terms. (http://www.w3.org/P3P/)

such as warranty cards and mall surveys. And others refuse to disclose how they collect information.[8]

These "people search" sites (and other privacy-implicating services) do not rely on the direct actions of a user to gather personal information; even a consumer who never used the Internet in her life would be vulnerable to these privacy practices. Many infrequent users of the Internet are shocked to find that their personal information has appeared online, despite never signing up for a social network or otherwise attempting to publicize it. Any consumer who votes, buys or sells real property, forwards her mail, or just exists in the 21st century is forced into participating in these sites, often without her knowledge or consent.

Some of these "people search" sites have voluntarily made an "opt-out" mechanism available: a consumer can visit most "people search" sites and ask that his information be removed from public display. However, some sites make the process unduly burdensome by requiring consumers to pay a fee, or requiring consumers to verify their identity by faxing a copy of their driver's license (seemingly defeating the point of requesting more privacy).[9] The complexity of this process should come as no surprise: the "people search" websites have little incentive to make the process easy for consumers whose privacy is being threatened. The websites' target audience is not the affected consumer, and every consumer that removes his information means one less piece of information that could otherwise be sold to somebody else.

Even if there were standardized opt-out procedures, consumers would have no idea where to begin to clean up their data. A consumer's personal information might be found on hundreds of these sites, with no notice to the consumer nor centralized directory of all places where their data is used. And, as the Internet advances, there are sure to be new categories of sites that publicize personal information in unexpected ways.

Current regulatory proposals are inadequate to address these sites and similar privacy challenges. Consumers are unable to "vote with their mouse" by choosing to avoid sites like "people finder" sites. A "Do Not Track" system would not be adequate to allow consumers to express their preferences: consumers have no reason to visit these sites, and the data sold by "people

---

[8] For example, people search site ZabaSearch.com only reveals the following in its FAQ:

> "All information found using ZabaSearch comes from public records databases. That means information collected by the government, such as court records, country records, state records, such as the kind of information that becomes public when you buy a new house or file a change-of-address form with the United States Postal Service. More often than not, it's individuals themselves who put their own information into the public domain, without realizing they are doing so." (http://www.zabasearch.com/faq/)

[9] See, for example, the ZabaSearch opt-out instructions. (http://www.zabasearch.com/block_records/block_by_mail.php)

finder" sites is not collected through behavioral tracking. Nor would "privacy by design" principles help when sites are intentionally designed to publicize private information.

Instead, any privacy regime must create standards that empower a privacy economy to help consumers take back control of their personal information from "white pages" sites, data brokers, and future privacy-threatening sites. Consumers must be able to find their information, know where it comes from, and express their desire to keep their information private. At the same time, the privacy regime must allow legitimate innovation and positive uses of data for societal good, and allow uses that consumers find desirable.

The status quo should not be the future; reboot online privacy from first principles

Now is the time to reboot consumer online privacy and eliminate outdated and antiquated privacy systems by starting from first-principle basics.

Some proposals, including the Preliminary Report, call for entrenching "commonly accepted practices" that are currently in use. However, the popularity of a practice in the current advertiser-driven online world should not decide its merit. Instead, each privacy practice should be measured on its own merit rather than by the number of consumers who have tolerated it.

Consumers may have tolerated current practices simply because these current practices have been imposed by large advertising firms as a matter of *fait accompli*, to be revoked or edited only when consumer outrage reached the level of threatening new regulation. Advertisers have set the default rules online, and they set those rules to captures as much data as possible. The only limits on advertisers have come when consumer revolt grew so loud that new regulation was threatened, at which point advertisers dialed-back the rules as little as possible to satisfy consumer demand. Most consumers simply accept the default settings online simply because it takes too much effort to find an alternative. It should be no surprise that advertisers want to collect as much data as possible: they have nothing to sell but data, and their massive storehouses of data about customers serve as a large barrier to new entrants. The result is that advertisers' current privacy policies are designed to collect and store as much data as consumers will tolerate without revolt.

Similarly, consumers have not had time to become informed about every offensive current practice, and advertisers have simply concealed many practices that may have privacy implications (such as the ability of marketing firms to gather data from companies like Rapleaf.com "behind the scenes" without directly notifying users). Consumers simply do not read multi-thousand-word

privacy polices, but cannot be deemed to have affirmatively "accepted" every practice in common policies today as a valuable practice that should be preserved or grandfathered.

Additionally, consumers may be accepting current privacy practices because they can't imagine an alternative system that might be superior. To take a familiar example in the history of marketing, the Sony Walkman is one of the most popular consumer devices of all time. But, prior to its introduction consumers never asked for a product like the Walkman because consumers did not yet have a vision of ubiquitous portable cassette music. Similarly, today, consumers don't realize that current privacy threats are not inevitable, and that other regimes are possible. For example, it might be possible to have a Facebook that does not store all of a consumer's personal information on Facebook-controlled servers,[10] but most consumers don't realize that such a privacy-protective system is technically feasible.

The fact that consumers grudgingly tolerate a policy does not mean that it should be solidified as a "commonly accepted practice," especially when consumers are not aware of all privacy practices or are not aware of alternatives. Instead, the Commission should use this opportunity to set rules to gather the "right" amount of data, or at least empower consumers to respond more effectively as technologies and data practices change.

Careful regulation will enhance innovation

By regulating basic privacy-protective principles and bringing appropriate enforcement actions, the Commission will enhance online innovation. Innovation is currently limited due to many difficulties: consumers are afraid of sharing data (or even of interacting online at all), legitimate businesses don't know how to properly handle data, and scammers exploit the regulatory uncertainty to utilize unsavory business practices. The only winners in the relatively unregulated field are those companies which are racing to the bottom the fastest; and consumers are of course the losers.

A true reboot of privacy will support innovation in all fields, especially if it starts from first principles rather than from entrenched industries. By giving consumers the tools to make their own informed privacy choices, and by empowering new privacy-protective businesses like Reputation.com, a new privacy economy will be created. The innovation that results will be far greater than any possible innovation in online advertising: behavioral advertising is a mature field with little room left for innovation when compared to the vast new market of privacy-protective products and services. It is true that advertisers would like to prolong the current system of

[10] The "Diaspora Project" was intended to solve some of the data centralization problems of Facebook by allowing data to be stored on distributed "nodes" that users could control, but it has yet to achieve meaningful marketplace success. See https://joindiaspora.com/.

behavioral advertising as long as possible, or to set default rules in favor of behavioral advertising, but as the comments to this Preliminary Report show, consumer sentiment is focused on taking back control of their own privacy. To the extent that sensible regulation affects the data collection for behavioral advertising, it is a good exercise for advertisers to determine if they can still create highly-relevant advertising without collecting intrusive personal information. It is likely that innovative solutions will be found that allow users to see relevant advertisements without giving up control over their personal information. And even if behavioral advertising is somewhat affected, behavioral advertising makes up a relatively small proportion of the total future innovation in online technology.

True innovation and privacy protection are synergistic. Each supports the other, in an increasing cycle of new technology that supports privacy, which encourages more use of Internet tools, which encourages new technology to support privacy, and so forth. If given the proper incentives, then new businesses can create new technological means to anonymize data, to store data in secured containers, to attach meaningful restrictions on the use of data, and more. The market has already invented at least one such service: the patent-pending "uProtect.it" application empowers consumers to choose how much data to share with Facebook.com, by offering consumers the option of storing their Facebook messages in an encrypted container outside of Facebook's servers; users are thus empowered to make sure that Facebook is respecting their data privacy choices.[11] Other innovative services will be created by many entrepreneurial companies as the privacy economy grows.

Trusted privacy advocates are the keystone of the privacy economy

Trusted privacy advocates are at the heart of innovation in the privacy economy. Privacy advocates include companies like Reputation.com and not-for-profit organizations such as the EFF and EPIC. These groups are working to build solutions for consumer privacy that help consumers understand their privacy more clearly and make informed decisions based on their unique preferences.

One of the largest problems that privacy advocates are working to solve is the sheer volume of privacy choices faced by consumers. Consumers have expressed interest in increased control over their personal data as it appears across hundreds of websites and data brokerages. Consumers are concerned about everything from their Facebook information, to behavioral ad tracking, to the profiles that appear on "white pages" sites, to how data brokerages sell information about them to offline marketers. Some consumers are aware of Facebook privacy settings, other consumers have

[11] See http://uProtect.it for more information. The service is powered by Reputation.com.

opted out of Google's ad tracking system, and others still have removed themselves from "white pages" sites. But few consumers are aware of all the ways that data is used online, and almost none have visited hundreds of sites in order to read and analyze the privacy policies they might find. In short, consumers feel overwhelmed by the number of places their information appears, and have no idea where to start to remove it all.

Trusted privacy advocates have emerged to bridge the gap between consumers' privacy interests and their knowledge. Companies like Reputation.com offer products and services which allow users to find how their personal information is distributed online and then exert control over it. These privacy advocates increase efficiency by centralizing knowledge: each advocate is an expert in identifying the thousands of websites that use personal data online, and can share that information with clients. For example, there is no reason for clients to spend tens (or hundreds) of hours researching every white pages site, analyzing its privacy practices, finding its opt-out mechanism, and then requesting to be opted-out. Instead, consumers can describe their preferences broadly and designate a privacy advocate to perform these steps on their behalf. The same goes for other forms of online data: social networking privacy settings, mailing-list companies, data brokers, behavioral ad tracking networks, and more.

The success of companies like Reptuation.com proves the viability of the privacy economy

Even in the absence of comprehensive baseline rules, there is already extensive evidence that the privacy economy is beginning to empower consumers to take control of their privacy. Private companies like Reputation.com have filled a recognized market need.

The speed of Reputation.com's growth is a testament to the demand for privacy. The company's "MyPrivacy" service is used by consumers worldwide as a privacy dashboard. The service shows consumers where their personal information (such as their name, address, phone number, and more) can be found online, and then gives consumers the opportunity to remove it with just a click. Consumers don't need to research each site that might contain their information, nor do they need to go through extensive opt-out procedures. In addition, the service allows consumers to remove themselves from more than 3,000 catalog and direct mail lists, as well as to set a global preference to opt out of behavioral advertising from some of the largest advertising networks in the world. Consumers can use the tool to understand their privacy choices, and then set the preferences they want: some prefer to opt-out of only behavioral tracking, some choose to opt-out only from people finder sites, and others are content with the status quo. This tool was developed though American innovation and entrepreneurship: a research team based in Redwood City, California developed the system without any need for taxpayer subsidy.

In fact, technological innovation in the privacy economy can create new jobs and increase tax revenue. Since its founding in 2006, Reputation.com has built a California-based team of engineers, research scientists, and other high-quality professional positions.[12] Other privacy economy concerns have also created other new technology-driven American jobs. Innovation in privacy-protective technologies will generate job growth and increase economic activities far more than further strip-mining consumer data ever could.

The future of privacy dashboard tools will be even more powerful if the right conditions are established to support an innovation-driven privacy economy. Innovative companies like Reputation.com and others will create the next generation of privacy-empowering tools that help consumers understand their online privacy and exert their privacy preferences.

Broad privacy rules will support a powerful privacy ecosystem

The government can most effectively promote consumer privacy by creating and thoroughly enforcing baseline rules that will support innovation and consumer empowerment in the new privacy economy. Rules that empower the principles below will create a flexible system that is capable of responding to new and unanticipated privacy threats created by new technologies or businesses.

The principle of clarity

Consumers should be able to clearly know how their data is being used, by whom, for what purpose, and how to correct it. This principle applies equally to sites that collect data from consumers directly (such as behavioral ad tracking network) and sites that collect data about consumers from other sources (such as "people finder" sites).

As many other comments have suggested, improving the depth and clarity of website privacy policy disclosures is a key goal. The form of these improved disclosures can take any of the forms suggested by other comments, and may vary based on the industry (e.g., it might be appropriate for consumer-oriented sites to display privacy icons, while expert-oriented sites have more nuanced terms of use).

As to sites that publicize personal information, such as "people search" sites, consumers are currently baffled as to how to prevent their information from appearing in these directories. Many people search sites give a few examples of their data sources, no sites currently provide consumers

[12] Reputation.com now employs more than 100 people at its headquarters in Redwood City, California. These high-quality knowledge-work jobs are the ideal source of sustainable economic growth in the 21st century.

any way to find out which data sources led to which records being displayed online. A consumer who prefers that her information not be online (or wants to correct erroneous information) has no idea which records to address to resolve the problem (and most people search sites say that the only way to correct the data displayed is to correct the underlying record). The introduction of a ground rule requiring clear disclosure as to the sources of information that go into an online profile will help consumers make better privacy choices, as well as help viewers understand the quality of and freshness of the data displayed.

The principle of control

Consumers should be able to decide *who*, *how*, *where*, and *why* their personal information is used. Of course, some businesses might require personal information to process transactions or provide other benefits: consumers should be able to make informed decisions about whether to allow use of their personal data or to not patronize that business.

This principle should apply to all actors in the data ecosystem, and enforcement actions should be brought against any violators. Additionally, consumers should be granted an opportunity to restrict "legacy" data that was granted before online privacy and data-mining became a concern; that data is being used in new and unexpected ways.

The principle of choice

Consumers must be able to choose how much or little privacy they want. There is no such thing as a privacy-neutral default setting; every privacy setting has privacy consequences and consumers must be able to choose their privacy. Privacy is a matter of taste and individual choice, and, accordingly, any solution to online privacy needs to empower consumers to express those choices. A privacy economy will provide the tools that consumers need to easily exert their personal privacy preferences, rather than a single setting chosen by business or government.

Consumers must also be empowered to make as general or as granular choices as they want: some consumers might want to keep all their data private, but other consumers will have different preferences for different types of data. For example, a man battling prostate cancer might want to keep his healthcare information private, while not minding if his address and phone number are publicly available. In contrast, a woman who has been stalked by an abusive ex- might not mind if her health profile is used to target advertisements for her, but might care passionately about making sure that her new address and phone number are hidden from public view.

The principle of accuracy

Consumers should be able to verify the accuracy of data collected about them, especially if it is being used to make decisions or offer special discounts to some consumers. Even consumers who are content with their data being shared or displayed in some cases may be shocked or offended when inaccurate information about them is publicized; for example, many consumers have found that "people search" sites have listed inaccurate political beliefs, religious affiliations, income levels, and more.[13] Other users have commented on the inaccuracy of behavioral tracking systems: Google's "Ad Preferences" page allows users to see at least part of the profile that Google has created based on a user's web history, including their supposed gender and interests (http://www.google.com/ads/preferences/). Many consumers have reported that the data is only partially accurate, suggesting that automated systems may be creating large volumes of inaccurate data. An effective solution will allow consumers to find inaccurate or incomplete data, and then to decide whether to delete it or correct the record.

The principle of revocability

Another suggested ground rule is the revocability of data. Permission to use data should be considered a lease rather than a sale; consumers may take back their data after the passage of time, and especially if the website has breached its promises about how it would use that data. Consumers should not be able to permanently alienate their right to privacy without clear and convincing evidence that they intended to do so; generally, a simple TOS or privacy policy at the bottom of a page would be insufficient without a commercial transaction.

Consumers often face difficulty fully understanding the consequences of giving their personal information (whether through their intentional acts or through a behavioral profile) to websites. The site may use data in an unexpected way, collect data in a surprising fashion, or periodically change its privacy practices: consumers must be empowered to revoke consent to use their data if a site changes its policies or practices. This would not be a major change: some major advertising networks, such as Google's AdWords program, already allow users to see the behavioral information that has been collected about them, and to retroactively revoke permission to use that information to target advertisements. In some cases, it may be impossible to fully retract or delete data, but to the extent technologically possible consumers must be empowered to take meaningful control of their data and the use of their data.

[13] Mark Hachman, "Spokeo Suit Claims Site Offers Inaccurate Information," PCMag, July 20, 2010 (http://www.pcmag.com/article2/0,2817,2366757,00.asp).

The principle of ease

Consumers should be able to make their own privacy choices with as little effort as possible. Consumers should not have to read lengthy multi-thousand-word privacy policies, sort through extensive procedures to "opt-out" from data collection, or go to heroic lengths to protect their data. Instead, it should be as simple as technologically feasible to empower consumers to express their privacy preferences. And, as technology advances, that should become significantly easier. By creating baseline regulations that encourage privacy innovation, consumers will benefit from new privacy "dashboards" and "control panels" that allow at-a-click control over their privacy choices across the Internet. One such emerging "control panel" is the MyPrivacy system from Reputation.com, which allows consumers at-a-click access to control over behavioral advertisement tracking, "white pages" sites, commercial email solicitation, and physical direct mail. Other privacy-enhancing innovative systems will grow as the privacy economy expands.

The principle of delegation

Consumers should be able to appoint trusted privacy advocates to exert preferences on their behalf. Just as there is no doubt that consumers can appoint technological agents to express their privacy preferences (such as a browser plug-in that automatically sends a "do not track" message to websites), consumers should be able to use a mix of technological and non-technological privacy advocates to do the work of protecting their online privacy. There is no need for consumers to become experts in working with the hundreds of data brokers, white pages, and other online information sites when a small cadre of skilled professionals can do this work far more efficiently. This simple condition will lay the groundwork for further innovation in privacy as technological and non-technological solutions are developed by the free market to help users express their privacy preferences.

The principle of flexibility

Current regulations cannot anticipate all possible sources of data, uses of data, or business models. As an example, the "Do Not Track" system is a technological improvement that will help consumers manage their privacy. But current visions of the "Do Not Track" system are specific to desktop browsers, and do not fully address the growing crisis around mobile and "app" data. An increasing proportion of "online" usage is through downloadable applications ("apps"), whether on the desktop through frameworks like Adobe Air (used to run apps ranging from stock tickers to Twitter clients), or on smartphones such as the iPhone and Android range. As the importance of mobile and "app" data grows, any baseline regulations will have to expand to address consumer concerns in those areas as well.

At the same time, the growth in technology and understanding can render current solutions inadequate. A privacy rule to limit behavioral advertising today might not work in the future when more data is available and there are more powerful algorithms to process it. A powerful example will likely arise in the next few years as facial recognition technology becomes even more mainstream. Right now, there are billions of photos online. Sometimes, the people depicted are identified, but in many cases they are not (often because they are bystanders, or in an attempt to protect the privacy of people depicted, or simply because there is no reason to identify them). Today's regulations cannot anticipate all such future uses, and any regulation should be a based on broad principles of consumer control that can be adapted regardless of the particular technologies that affect privacy.

Conclusion: Reboot consumer privacy and let the new privacy economy bloom

Innovative combinations of technology and regulation, such as the "Do Not Track" system, can solve immediate concerns regarding behavioral ad tracking. However, these rules are not enough to sustain long-term consumer privacy empowerment. Instead, a broad set of privacy principles, backed by appropriate regulation and powerful enforcement, will create a framework that will adapt to future technologies and privacy threats. Consumer empowerment will be maximized by starting from first principles rather than further entrenching that status quo; simply because some privacy practices have been ignored or tolerated does not mean that they are the ideal for consumers.

Using these broad principles and careful enforcement actions, the Commission can empower the competitive market to create powerful and taxpayer-efficient solutions to complex privacy problems. The blossoming privacy economy also has the advantage that it respects consumer preferences for privacy or publicity: there simply is no neutral "default setting" for privacy, and instead consumers will turn to innovative privacy tools that help them express their privacy preferences. The privacy tools that meet consumers' demands and allow expression of particular preferences will become popular, while those that do not will disappear or be forced to adapt. With simple baseline rules, such as clear disclosures by websites and the ability of consumers to delegate their preferences to privacy advocates, the privacy market will provide a powerful and flexible solution for future privacy needs.