



Before the
United States Department of Commerce
National Telecommunications and Information Administration

Comments of
Reputation.com, Inc.

Responding to the Notice of Inquiry

regarding

**“Commercial Data Privacy and Innovation in the Internet
Ecosystem”**

Docket # 101214614-0614-01

January 28, 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 Commerce Department’s Notice of Inquiry regarding its report, “Commercial Data Privacy and Innovation in the Internet Economy.” 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.

Introduction

Consumers face great anxiety and confusion over their online privacy. They fear that their personal information—ranging from their search terms, to the links they click on, to their home address, to their photos—will be shared or mis-used without their permission. Consumers are frightened by their personal information showing up on so-called “people finder” and “white pages” sites,¹ by their data being used to target offline solicitations, and by offline records being made accessible to anyone in the world with an Internet browser. Consumers have differing preferences as to their privacy, but often don’t know where to begin to solve their privacy needs. Regulators and government agencies face a difficult challenge identifying means to address these problems without stifling legitimate innovation. And legitimate businesses tread lightly, lest they be incorrectly accused of privacy violations.

Despite these obstacles, hope is not lost. Consumer online privacy can be improved by carefully stoking the fast-growing privacy economy. The privacy economy is already empowering consumers to take back control of their personal information, and giving consumers the tools they need to make informed decisions about their privacy. American innovation is one of the most productive forces on earth, and with careful structural help it can be applied to solve the complex problems of online privacy. By clearly delineating and enforcing some basic ground rules, the government can create the infrastructure for pro-privacy innovation and entrepreneurship to flourish. New jobs will be created, new technologies will be developed, and the economy will expand.

If properly implemented, the Dynamic Privacy Framework could be an effective step toward this form of consumer empowerment. The Dynamic Privacy Framework, viewed as a combination

¹ Such as Spokeo.com, WhitePages.com, ZabaSearch.com, PeopleFinder.com, PeopleFinders.com [sic], Pipl.com, iSearch.com, and many others.

of Fair Information Practice Principles (“FIPPs”) and enforceable codes of conduct can be an effective step toward addressing consumer privacy concerns. By enhancing the ability of consumers to understand the ways that their data is being used, and by creating select few ground rules that will cover basic principles rather than specific technologies, the Dynamic Privacy Framework will lay the foundation for a privacy economy that will grow to meet the privacy challenges faced by consumers.

Comprehensive online privacy solutions need to address multiple classes of privacy relationships

Much recent attention has focused on the privacy impacts of behavioral advertising and similar technologies. Behavioral advertising is based on tracking a user’s behavior (such as search queries, clicked links, and more) across one or more sites with which they are interacting. At the core of behavioral advertising is a “direct” relationship, in that the consumer is interacting with the website that might impact the consumer’s privacy. The relationship is also “direct” in that the data used to customize advertisements is gathered directly from the consumer’s interactions. For example, a social networking website might gather information that a user voluntarily inputs into the social networking website, and use that to customize the content that is displayed. Or, a behavioral ad tracking network might gather data by placing a cookie on a consumer’s computer, and then periodically reading the cookie as the consumer browses from site to site; at each moment the cookie is read, the user’s web browser is interacting directly with the advertising network.

In other words, in direct privacy relationships, the consumer is the source of the privacy-sensitive information, and has some opportunity to choose to not interact with websites that do not respect the consumer’s privacy. As we will discuss below, there is ample opportunity for technology and regulation to improve the privacy experience of consumers by making it easier for consumers to understand how data is being collected and to express their own preferences in response.

But these “direct” relationships are not the only sources of privacy concerns online. 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 consumers have been disturbed by these perceived violations of their privacy. The names of the “white pages” websites have been redacted, but the comments are representative of consumer reactions to several “white pages” and “people finder” sites:

“[REDACTED] can be freakishly frightening. I put in an old email address and it pulls up my old address on Google Earth!” – Twitter user Anthony Shelley (“anthonyshelley”), January 25, 2011.²

“Yall gotta go to [REDACTED].com and type your email or name.. its scary how much of your personal info is on there... this is not a joke!!!!” [sic] – Twitter user “OfficialAlexTV,” January 24, 2011.³

“Remember how you don't post your info online? Now it's not your choice. Make the choice to remove your info from [REDACTED].com” – Twitter user “adorablepuppy,” January 26, 2011.⁴

“[A] first encounter with [REDACTED].com is spooky. How could a website know where I live, how many individuals are in my family, the value of my home, and so on? It's just plain creepy.” – Blogger Dan Dunlop, January 25, 2011.⁵

“[REDACTED].com really is a well-designed stalker tool” – Twitter user Geoff Alday (“geoffa”), January 23, 2011.⁶

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, such as warranty cards and mall surveys. And others refuse to disclose where they get their information.⁷

Importantly, these people search sites do not rely on the direct actions of a user for their data; even a consumer who never used the Internet in her life would be vulnerable to these privacy

² <http://twitter.com/anthonyshelley/status/29956886128230400>

³ <http://twitter.com/OfficialAlexTV/status/29757162699890688>

⁴ <http://twitter.com/adorablepuppy/status/30202968863150081>

⁵ <http://thehealthcaremarketer.wordpress.com/2011/01/25/spokeo-is-spooky/>

⁶ <http://twitter.com/geoffa/statuses/29378209699069953>

⁷ 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/>)

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 their personal information. 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 indirect sites, often without her knowledge or consent. And unlike the old phone-company “white pages” directory, consumers have no idea who to call to fix the problem.

These “people search” sites are the most visible distant privacy sites today, but there are many more involuntary data flows than many consumers realize. For example, a company called Rapleaf allows marketers and e-commerce sites to lookup a user’s name, gender, age, ZIP code, interests, number of children, and marital status—instantly and on demand.⁸ A website can access this data from Rapleaf just with an email address from a consumer; possibly under the guise of asking a consumer to join a mailing list or requiring a consumer to receive a password by email. This data can be used by commerce websites to decide which customers see which prices, or to deny access entirely to certain disfavored customers. Other sites may use it to provide discounted deals and specialized content to only members of certain demographic groups. This all goes on “behind the scenes,” often without the consumer’s knowledge.

Even social networking sites like Facebook are also collecting distant privacy data. Social networking sites can gather a huge amount of information about a consumer without that consumer’s involvement. For example, a Facebook user might provide the minimum possible information about herself, but her friends will provide vast amounts of information about her to Facebook when they “tag” her in photos, when they mention her in “notes” and “status updates,” and even by the act of “friending” the consumer in the first place. Facebook recently increased the amount of information it collects by adding a geo-location feature: when a users “checks in” to a place (i.e., announce to friends that he is at bar, club, or restaurant), Facebook asks that user if there are any other users present. If the user enters the names of his fellow bar-goers, then Facebook has collected geo-location and habit information about those fellow bar-goers, without their consent or knowledge. (And Facebook’s ever-evolving privacy practices increase concern that it may mis-use this data: until public backlash grew too strong, Facebook attempted to provide users’ phone numbers with Facebook app developers with no chance to opt-out).⁹

⁸ Source: Rapleaf API description.
(http://www.rapleaf.com/developers/api_docs/personalization/direct#example_json_response)

⁹ Violet Blue, “Facebook Gives Apps Your Phone Number and Address, No Opt Out,” ZDNet, January 17, 2011 (<http://www.zdnet.com/blog/perlow/updated-facebook-gives-apps-your-phone-number-and-address-no-opt-out/15555>).

Of course social networking and “people search” sites still might be socially positive if their privacy implications are adequately addressed. Just like the old hardcopy telephone “white pages” directory, “people search” sites provide a valuable service by making it easier to find and connect with long-lost friends and acquaintances. Many consumers are not bothered by the presence of their personal information on these sites, and others actively support it. But for the remainder of consumers, their privacy is severely harmed by these sites. For a domestic abuse survivor, every “white pages” site is another way for an abusive ex-spouse to get back in touch. For federal officials, publicity surrounding their address and family information can be dangerous in the current partisan environment. Others simply prefer that their very private information not be exposed. And unlike the old print “white pages” directory, many consumers don’t know how to remove their information from these sites. An effective privacy solution requires empowering consumers to easily control the distribution of their personal information, especially with respect to sites with which they have not interacted.

Direct privacy relationships can be enhanced through negotiation-enhancing FIPPs and technologies

Consumers’ privacy experiences in direct privacy relationships can be improved by enhancing the ability of consumers to understand the privacy tradeoffs they are making, and by helping consumers express their preferences more easily. Technology, improved privacy practices, and innovation can all assist consumers in asserting their preferences.

Direct privacy relationships resemble contractual negotiations: a website offers certain features in exchange for accepting its privacy terms. Consumers may visit the website and accept the privacy terms, or consumers may request different terms by asking to opt-out of certain tracking features. Alternatively, consumers may decline a site’s privacy terms by abstaining from visiting the site, thus keeping their data out of unwanted hands.

However, it is difficult for consumers to negotiate their privacy-related concerns. It is time-consuming for consumers to find and understand the privacy terms of tens or hundreds of sites per day: one recent study found that the average privacy policy was 2,500 words long and would take more than 10 minutes to read.¹⁰ Facebook’s privacy policy is more than 5,500 words long as of this writing, which would take an average consumer more than 20 minutes to read in full.¹¹ (The privacy policy is in addition to 3,900 words of general terms and conditions, 1,600 words of special terms

¹⁰ Out-Law, “Average Privacy Policy Takes 10 Minutes to Read, Research Finds” June 10, 2008 (<http://www.aleecia.com/press-coverage/outlaw.pdf>).

¹¹ Facebook, “Facebook’s Privacy Policy,” December 22, 2010 (<http://www.facebook.com/policy.php>).

for users who make purchases on the site, and more than 500 additional words of non-binding “Facebook Principles.”) 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. For example, Facebook’s privacy settings page offers users more than 20 different privacy settings, each with up to five options to select from. Consumers are simply overwhelmed.

In the absence of easy methods to express privacy preferences, some consumers have resorted to brute-force technological methods to exert their preferences: consumers can delete tracking cookies, or can use browser plug-ins to block offensive advertisements.¹² Other consumers intentionally send misleading behavioral data, in an attempt to disguise their actual preferences behind other behaviors.¹³ And consumers can also simply choose to not visit sites with unfavorable behavioral advertising practices; an effective form of voting with one’s mouse.

Technology and improved practices can reduce friction in privacy relationships and make it easier for consumers and sites to negotiate. Additional ground rules and FIPPs will empower a privacy economy in this space.

Some research has focused on reducing friction by making it easier for consumers to understand the privacy policies of sites they visit. For example, there have been proposals for standard graphical privacy icons¹⁴ or machine-readable privacy terms¹⁵, that allow consumers to quickly understand how their personal-information will be used by a given site. These fact-gathering tools reduce the time consumers spend reading the privacy terms and conditions of the tens of websites they visit every day. Instead of reading a complex legalistic privacy policy, consumers can glance at standardized terms and quickly decide if a particular site meets their privacy expectations. 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 sites.

¹² For example, the Adblock Plus plug-in for the Firefox browser allows users to reject all, some, or certain types of advertising from being displayed.

¹³ For example, the aptly-named “TrackMeNot” browser plug-in periodically runs random searches on search engines in order to create misleading behavioral preferences. (<http://mrl.nyu.edu/~dhowe/trackmenot/>)

¹⁴ 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>)

¹⁵ 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/>)

Other research has focused on reducing friction by making it easier for consumers to express their privacy preferences to websites. These communications tools standardize consumer responses to privacy practices, so that consumers may consistently communicate their preferences. For example, the browser-based implantation of a “do not track” header is simply a way for consumers to communicate a tracking preference to all sites they visit.¹⁶ In turn, the sites they visit may choose to accept the consumer’s proposed terms (no tracking), or reject the visitor and inform her that tracking is required to use certain 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. Automated communication is especially more effective 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.¹⁷ Consumers simply don’t have the time to express their preferences to 168 different tracking tools, but a browser “do not track” feature will automatically handle the communications before a web page even fully loads.

Other private-sector tools also allow consumers to declare their preferences. Some private services, such as Reputation.com’s “MyPrivacy” service, include the option to set a browser cookie that serves as a flag recognized by major behavioral advertising firms.

But these interactions could be further improved by the continued growth and support of the privacy economy. By laying clear ground rules, discussed below, it will be possible to further empower consumers to make informed choices about their privacy.

Distant privacy relationships require enhanced consumer involvement

Distant privacy relationships present a very different problem. Consumers are unable to “vote with their mouse” by choosing to avoid sites like “people finder” sites. Every consumer’s data is part of these sites by default, whether or not the consumer has ever interacted with the sites. And the privacy violations can be far more intrusive: consumers often find their home address, names of family members, creditworthiness, approximate income, previous addresses, and more—all displayed publicly for anyone to see.

¹⁶ See, for example, Jonathan Mayer and Arvind Narayanan, “Do Not Track: Universal Web Tracking Opt-Out” (<http://donottrack.us/>).

¹⁷ 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>).

Some sites that distribute personal information gathered from distant privacy relationships (including many “people search” sites) have voluntarily made an “opt-out” mechanism available. Any consumer can visit a “people search” site and ask that his information be removed from public display; most people search sites will comply with the request. However, some sites make the process unduly burdensome by requiring consumers to pay a fee, or requiring consumers to verify their identity by providing a photocopy of their driver’s license (seemingly defeating the point of requesting more privacy).¹⁸

In these cases, the offensive websites have little incentive to make the process easy for consumers whose privacy is being violated: 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.

Equally importantly, consumers have no idea where to begin to clean up their data. In the case of direct privacy relationships, consumers can start to understand their privacy by inspecting the privacy policies of the sites they visit. By using tools such as “do-not-track,” consumers can express their preferences to sites as they visit, or sometimes consumers can return and retroactively delete privacy-sensitive data. But a consumer’s personal information might be found on hundreds or thousands of indirect sites, with no notice to the consumer. There is no centralized directory of all data brokers, nor of “white pages” sites. And as the Internet advances, there are sure to be new categories of sites that publicize personal information in unexpected ways.

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, leading to at least one lawsuit.¹⁹ Users have been embarrassed when people search websites proclaim that they hold the wrong religious or political beliefs, or suggest that they are poorer (or richer) than they actually are. Other users have commented on the inaccuracy of behavioral tracking systems: for example, 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

¹⁸ See, for example, the ZabaSearch opt-out instructions.

(http://www.zabasearch.com/block_records/block_by_mail.php)

¹⁹ Mark Hachman, “Spokeo Suit Claims Site Offers Inaccurate Information,” PCMag, July 20, 2010 (<http://www.pcmag.com/article2/0,2817,2366757,00.asp>).

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.

Unlike in direct relationships, it is not possible to empower consumer privacy as to indirect relationships simply by making negotiation easier. 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-invasive distant 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 users that consumers find non-objectionable.

An empowered privacy economy can solve these complex privacy problems

Online privacy presents complex problems: consumers have varying tastes for privacy, there are a huge number of interested parties (ranging from millions of consumers to thousands of advertisers to hundreds of data brokers), many consumers are unaware of the risks to their privacy, and there are no standards in place for most communications between parties. But an empowered privacy economy can create the right incentives for cooperation and productive solutions that encourages pro-privacy innovation, creates jobs, and gives control back to consumers.

An empowered privacy economy consists of a mixture of sensible government baseline rules, enforcement of FIPPs, and entrepreneurial private actors who close the loop between consumer education, consumer preferences, and implementation of those preferences. Each part is necessary to create a privacy regime that encourages innovation, gives consumers the control they want, and builds American jobs.

A privacy economy will expand protections beyond narrow sector-specific privacy laws

The current sector-specific laws (such as HIPAA and the Fair Credit Reporting Act) are a good start in that they prevent some egregious abuses and call attention to certain socially-unacceptable policies. But they are insufficient in that they don’t cover all current undesirable practices, let alone possible future misuses of data.

To take HIPAA as an example, it is a powerful law that protects sensitive consumer health information. Under HIPAA, it would be illegal for a hospital to publicly disclose a patient’s

treatment information. However, HIPAA's protections extend only to data that is released by healthcare providers: doctors, hospitals, healthcare plans and a few others.²⁰

Nothing in HIPAA would stop a company like Google from secretly selling a list of people who have searched the web for cancer-related information (think of search terms like “mammogram false positive”, “mastectomy”, or “cancer centers near Washington, D.C.”). A list of people searching for information about a cancer diagnosis would be invaluable to health and life insurers, as it would allow them to quickly eliminate the most expensive consumers from their risk pools. Even if insurers were unable to directly drop “cancer risks” under pre-existing-condition rules, creative insurers could discourage cancer risk patients by not marketing to them or even by driving at-risk consumers toward negative information about coverage denials. There would undoubtedly be an uproar if such practices were to be discovered, but nothing in HIPAA would prevent the data from being shared. (Of course, there is no reason to believe that Google currently sells such information, but nothing prevents a less-scrupulous company from doing so.)

Similarly, nothing stops Facebook from selling a list of names of probable cancer patients based on their status updates and geo-location check-ins (such as users who are spending a lot of time near hospitals). Or Facebook could even use *indirect* data generate the same list of at-risk consumers: even if a consumer does nothing online related to her cancer treatment, she could still be revealed by a friend's message saying “good luck at chemo tomorrow!” or “I'm praying for your lump to be harmless.”

Of course, there is nothing about these examples limited to cancer and health insurance. These examples could just as easily apply to drinking alcohol (check-ins at bars or searches for “happy hour specials”) and auto insurance, or to trips to Las Vegas and mortgage rates. It is simply impossible to predict every possible mis-application of consumer data, and legislators would be left to play “Whac-A-Mole” as new data abuses popped up in new sectors. Instead, the problem is best addressed by broad baseline rules that let consumers select what areas of privacy are most important to them, and a regime that encourages private implementation and enforcement of these preferences.

A privacy economy can provide relief when technological change is moving too fast for one solution

Just as sector-specific approaches are too limited, so are solutions tied to one technology. Much ado has been made in recent months over the implementation of a “do not track” header in

²⁰ 45 C.F.R. 164.501.

certain Internet browsers. The “do not track” header is a technological improvement that will help consumers manage their privacy. However, care must be taken to not give the false impression that “do not track” will solve online privacy. The “do not track” header is specific to desktop browsers, and does not 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. The “do not track” header does not address mobile or app data, nor any data created outside a traditional web browser.

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).

In the near future, facial recognition and the ever-increasing quality of cell phone cameras will allow privacy-invasive websites to collect even more involuntary information about consumers, without consumers even knowing it. Profile sites will be able to use facial recognition to locate photos of (and information about the habits of) consumers, without the consumer having any idea. For example, the site “Face.com” allows Facebook users to apply facial recognition to Facebook photos to identify their friends or enemies (even if the subjects have not been “tagged” in the photo or have removed their names from the photos). There is no technological reason why Facebook couldn’t run its own facial recognition software on all photos that users have uploaded, in order to identify social relationships of the people depicted—or create a list of people identified at politically-sensitive events (such as at an abortion facility) or potentially risk-sensitive places (buying alcohol, appearing intoxicated, participating in adventure sports).²¹ Today’s solutions cannot anticipate all such future uses, and any solution must adapt to the rapid pace of technological changes.

An effective privacy economy will empower consumer choice

An effective privacy economy encourages consumers to make their own choices about privacy. Some consumers prefer to increase their visibility online, going as far as to sign up on sites

²¹ In fact, evidence suggests that Facebook is already experimenting with automated facial recognition behind-the-scenes, and using other users to test the accuracy of its results. Helen A.S. Popkin, “Facebook’s facial recognition knows who your friends are,” MSNBC, December 16, 2010 (http://technolog.msnbc.msn.com/_news/2010/12/16/5660488-facebooks-facial-recognition-knows-who-your-friends-are-).

like LinkedIn that publicize their resume and contact information (or even publishing their phone number on their own “.com” website). Some consumers are happy to trade some personal information for a more tailored online experience, such as by entering their preferences and demographics into sites that suggest activities or movies, or by using a service like “Facebook Connect” to customize review sites like Yelp based on their friends’ activity. Other consumers are indifferent to these privacy concerns and accede to advertising personalized to their interests. And yet other consumers prefer complete control over their personal information and would prefer to never have their sensitive data stored, tracked, or shared online.

To further complicate matters, one consumer might have different preferences for different types of data. A man battling prostate cancer might care deeply that his healthcare information not be publicized or used against him, 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.

None of these preferences are innately better or worse than any of the others. Privacy is a matter of taste and individual choice. Any solution to online privacy needs to empower consumers to make their own privacy choices. A privacy economy will provide the tools that consumers need to easily exert their personal privacy preferences, rather than a single “one-size-fits-all” privacy setting imposed on a command-and-control basis.

Technological innovation can work in favor of privacy, and privacy will foster further innovation

There is no conflict between innovation and privacy. 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 *ad nauseum*.

Increased consumer confidence in the privacy and security of their Internet browsing will increase the number of consumers who are willing to use Internet tools and services. Right now, many consumers refrain from using rich Internet applications due to privacy fears. If their privacy concerns are addressed, there will be a larger critical mass of users willing to engage in rich online interaction, which will spur further substantive innovation into new and useful services that consumers demand. If online privacy can be solved, the next decade might see incredibly detailed immersive, and social applications that will enrich lives and boost the American economy.

To the extent that sensible regulation reduces the data available for behavioral advertisers to track consumers, it may be a good exercise for advertisers to determine if they can still create highly-relevant advertising without collecting as much personal information. It is likely that innovative solutions will be found that allow users to see relevant advertisements without giving up 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. A properly-regulated privacy economy will dislodge entrenched interests and allow new innovation that will benefit consumers; the most valuable innovation will occur in privacy-protective technology rather than further refinement of behavioral advertising models and further strip-mining of consumer data. A truly sustainable Internet ecosystem will focus innovation instead on pro-consumer technologies that fill consumers' needs.

If a privacy economy is supported, many new innovative technologies will protect privacy at minimal cost. For example, "CAPTCHAs" (those questions that ask "what are the letters in this box?") were invented in the late 1990s. These tests are now frequently used to allow humans to access privacy-sensitive data, while banning other websites from "scraping" (automatically copying) it *en masse*.²² The goal of making information available to those with a legitimate need is fulfilled, while privacy-troubling mass copying is prohibited. If a market is created that will value them, then future innovations will empower legitimate uses of privacy-sensitive data while preventing abusive uses.

More recent privacy innovations have been created by companies leading the privacy economy. For example, Reputation.com recently launched a patent-pending privacy tool called "uProtect.it" which allows Facebook users to post encrypted messages that Facebook itself cannot read. This tool prevents Facebook from using personal messages to create a behavioral profile, and reduces the risk to consumers in case Facebook ever suffers a data breach. Other innovative privacy technologies will emerge as the privacy economy continues to grow.

Trusted privacy advocates and pro-privacy innovators are the keystones 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

²² For example, many domain name registrars use CAPTCHAs to prevent automated access to "whois" data that lists the name and address of domain name owners. An individual interested in finding the owner of a particular domain can easily complete the CAPTCHA, but a computerized harvester cannot automatically collect thousands of email addresses to create a mailing list.

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 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 Reputation.com proves the viability of the privacy economy

Even in the absence of comprehensive baseline rules and FIPPs, there is already extensive evidence that the privacy economy is beginning to help consumers take control of their privacy. Private companies like Reputation.com have filled a recognized market need. With customers in more than 100 countries worldwide, Reputation.com has proven that there is a clear demand for innovative tools that help consumers understand their privacy. The market agrees that there is a future in the privacy economy: Reputation.com has received investments from world-leading venture capital firms including Kleiner Perkins and Bessemer Venture Partners.

Before the success of Reputation.com, some observers speculated that consumers would be unwilling to pay for privacy or exert effort to protect it. But consumers are already investing tens of thousands of hours of their own time installing software like AdBlock Plus and proxy software designed to protect themselves from behavioral advertising. Recent Gallup polls shows that many users would rather pay a fee to view online content than have their activities monitored.²³

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 advertisements, some choose to opt-out only from people finder sites, and others are content with the status quo. This tool was developed through American innovation and entrepreneurship: a research team based in Redwood City, California developed the system without any need for government intervention or 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 professionals.²⁴ Other privacy economy concerns have also built 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 behavioral tracking 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. And as these companies grow, they will increase employment and tax revenues.

²³ The Atlantic, "Most Internet Users Willing to Pay for Privacy," December 22, 2010

(<http://www.theatlantic.com/business/archive/2010/12/most-internet-users-willing-to-pay-for-privacy/68443/>).

²⁴ 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.

Baseline standards and FIPPs will support a powerful privacy economy

The government can most effectively promote consumer privacy by creating baseline rules that will support innovation and consumer empowerment in the new privacy economy. Such a privacy economy will allow consumers to easily make informed choices about their privacy, empower consumers to address both direct and distant privacy relationships, and boost the American economy through both direct and indirect job creation.

Basic privacy ground rules can empower the privacy economy

A few basic ground rules for privacy can support the privacy economy. The details of these rules can best be developed through further multi-stakeholder meetings, but several suggestions are given below for the sake of spurring further conversation.

As many other comments have suggested, improving the depth and clarity of disclosures is a key goal. Consumers must be able to understand the consequences of giving information to sites with which they are in “direct” relationships, and also understand the sources of data used by “people finder” sites and other “indirect” relationships.

To better understand direct relationships, improved clarity of disclosures would be helpful. Technological innovations (such as the free “Web of Trust” browser toolbar) can assist privacy by displaying community reviews of a site and its practices, but ultimately full disclosure must come from the sites themselves: even a tool like Web of Trust cannot detect behind-the-scenes data sharing that consumers might object to. 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 indirect sites, 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 (such as voting records), but do not inform consumers 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 update to resolve the problem. 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.

Another suggested ground rule is the revocability of data. 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. In many cases, it would be a fair business practice to allow consumers to know what information about them has been collected, and then revoke consent to its use if the data is wrong or just too invasive. Some major advertising networks, such as Google's advertising program, already allow users to see the behavioral information that has been collected about them, and to retroactively revoke permission to use that information. This practice should be expanded to give consumers the clear opportunity to see how their information is being used and then decide whether they permit further use. In some cases, it may be impossible to fully retract or delete data, but multi-stakeholder discussions can make clear the best ways for consumers to take meaningful control of their data and the use of their data.

Finally, a key principle should be that consumers can 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 cleaning up 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.

Conclusion: Let the privacy economy bloom

The competitive market is the most powerful and taxpayer-efficient way to create innovative solutions to complex privacy problems. There is little government spending or intervention required to create the conditions for a free and innovative privacy market. Instead, by simply putting in place some baseline rules and enforcing voluntary fair practices, the government can unleash the power of privacy innovators who will develop the next generation of privacy solutions, at no cost to the taxpayer.

The blossoming privacy economy also has the advantage that it respects consumer preferences for privacy or publicity. Those privacy tools which fill 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.