FUNG INSTITUTE
for ENGINEERING LEADERSHIP
UC BERKELEY COLLEGE OF ENGINEERING

Internet, Economy and Privacy

Anil Dagar,
Yasuhiro Endo,
Abhay Gupta,
Yan Li,
Kuldip Pabla ,
Sridhar Ramaswamy,
Ikhlaq Sidhu

College of Engineering
University of California, Berkeley

Fung Technical Report No. 2013.04.16
www.funginstitute.berkeley.edu/sites/default/files/Internet-Economy-and-Privacy.pdf

April 16, 2013

The Coleman Fung Institute for Engineering Leadership, launched in January 2010, prepares engineers and scientists – from students to seasoned professionals – with the multidisciplinary skills to lead enterprises of all scales, in industry, government and the nonprofit sector.

Headquartered in UC Berkeley's College of Engineering and built on the foundation laid by the College's Center for Entrepreneurship & Technology, the Fung Institute combines leadership coursework in technology innovation and management with intensive study in an area of industry specialization. This integrated knowledge cultivates leaders who can make insightful decisions with the confidence that comes from a synthesized understanding of technological, marketplace and operational implications.

130 Blum Hall #5580 Berkeley, CA 94720-5580 | (510) 664-4337 | www.funginstitute.berkeley.edu

Abstract: The Internet is a critical component of the global and domestic economy. The economic impact of the Internet on people's lives is difficult to estimate in terms of dollars, but online advertising is the dynamo powering the Internet's rapid growth. Internet advertising has grown dramatically over the past decade. Ensuring that online advertising revenues continue to grow will be central to the Internet's growth and success tomorrow. One way websites gain more value from online advertising is by providing more relevant ads, which will benefit both consumers who get more utility from these ads and advertisers who reach their target audience. Ads are targeted are based on information collected about users, which has raised a lot of fear. Several of the most recent privacy violations, security breaches and lawsuits have accentuated these fears. In this report we analyze the growing trend of new regulations, like the Do Not Track bill, that governments are trying to legislate to protect the rights of the general public. These new privacy regulations could reduce the effectiveness of online advertising and thus reduce the available revenue to support free or low-cost content, applications and services. This report further describes the anticipated business landscape changes and identifies various new opportunities.

1. Introduction: Internet Economy

The Internet is important to our economy and online advertising drives the Internet's rapid growth. Many of the websites that millions of Americans depend on for work and play would not be around today without online advertising. In fact, the top five websites in the United States (Google, Facebook, Yahoo, YouTube and Amazon.com) use online advertising to support their products and services.

Internet advertising revenues in the U.S. reached $9.26 billion for the third quarter of 2012, the biggest quarter on record according to 2012 IAB Internet Advertising Revenue Report [1] figures released by the Interactive Advertising Bureau (IAB) and PriceWaterhouseCoopers (PWC). In addition, they mark a 6 percent increase over the Q2 2012 figures of $8.72 billion.

"This uptick goes beyond a significant year-over-year increase at 18 percent, and also shows a climb from last quarter as well," said David Silverman, a partner at PWC LLP. "Clearly, digital advertising is continuing its positive trajectory with incredible momentum as it heads into seasonally strong Q4."

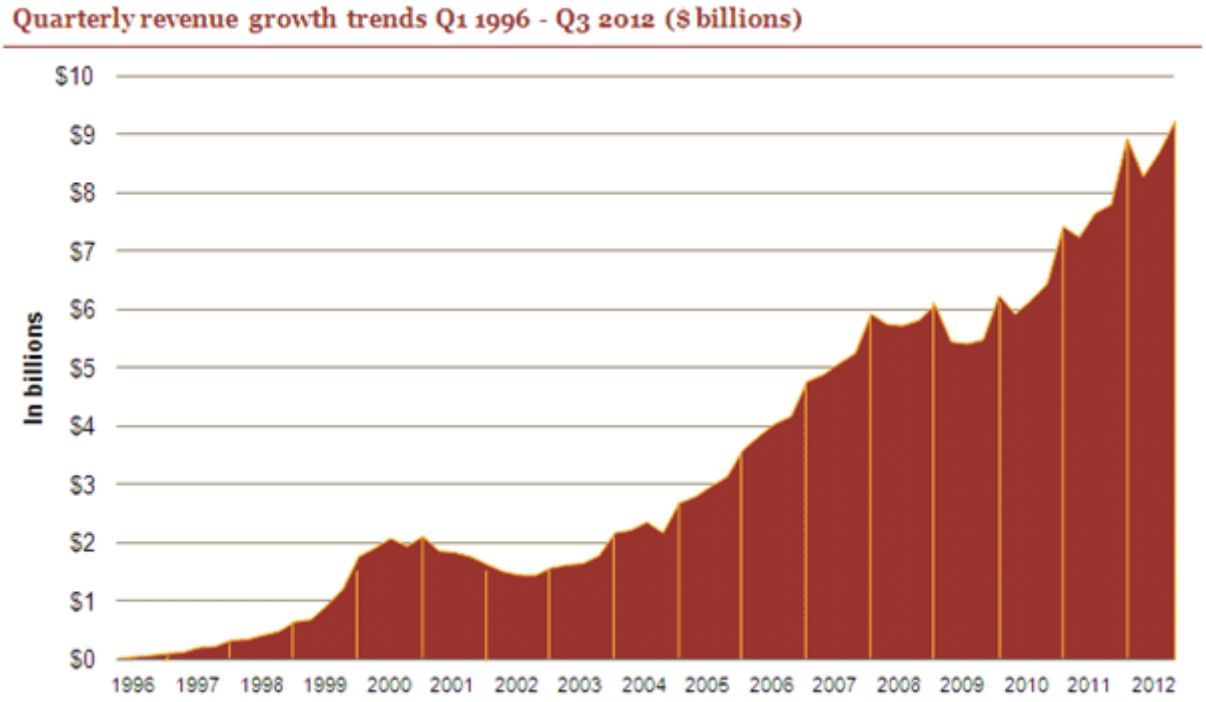


Figure 1: Internet Advertising Revenue Trends (Source: IAB)

If online advertising is important to the Internet ecosystem today then ensuring that online advertising revenues continue to grow will be central to the Internet's growth and success tomorrow. One way websites can gain more value from online advertising is by providing more relevant ads. Targeted ads benefit both consumers who get greater utility from these ads and advertisers who are willing to pay more to reach their target audience. Targeted ads, which are based on information about a user like browsing history or other user-specific data, help deliver higher-value ads.

Collecting user information for targeted advertising has raised a lot of fear and controversies, most particularly towards the privacy rights and policies. Privacy International is fighting to make

governments legislate to protect the rights of the general public. According to Privacy International, interception of web traffic must be conditional to explicit and informed consent from any ethical standpoint. Action must be taken where organizations can be shown to have acted unlawfully. Policymakers seem intent on imposing data privacy regulations that would limit the ability of Internet publishers to tailor advertising to users based on their interests.

1.1 Impact of Targeting Advertisement on Internet Economy

The Network Advertising Initiative conducted a study in 2009 [2] to measure the price and effectiveness of targeted advertising. It revealed that targeted advertising:

- Secured an average of 2.7 times the revenue per ad more than non-targeted "run of network" advertising.
- Was twice as effective at converting users who just click on ads into buyers

One might question what would have happened in the absence of targeting, since the users targeted by advertisers are more likely to convert than the general population. Farahat and Bailey measured the true economic impact of targeted advertising on brand searches and clicks. They found, assuming the cost per 1000 ad impressions (CPM) is $1, that:

- The marginal cost of a brand-related search resulting from ads is $15.65 per search, but is only $1.69 per search from a targeted campaign.
- The marginal cost of a click is 72 cents, but only 13 cents from a targeted campaign.

Targeted Advertisement is possible by tracking files, called "cookies," on users' computers and monitoring them as users browse the Web. Advertising networks then display ads tailored to users' browsing history. Privacy groups, lawmakers and regulators worried about personal privacy have called for restrictions on online tracking. A survey conducted in the United States in 2012 revealed that 68 percent of Americans are not fans of targeted advertising, but rather see it as invasion of privacy.

Online advertisers feel that this is due to misconceptions about how targeting advertising works. The following two examples illustrate this point:

- When Google offered ads to its Gmail users based on contextual information in emails, privacy advocates objected to Google "reading people's email." Yet these claims do not distinguish between ads delivered to these users through automated computer technology and an individual snooping through personal emails.
- A wedding photographer in Dallas can pay Facebook to serve an ad to everyone in Dallas who switches his or her relationship from "single" to "engaged". This benefits everyone – the photographer gets more clients, the users get more relevant ads. At no time does the photographer learn who sees the ads, unless the user chooses to make contact.

1.2 Impact of Privacy Regulations

Regulations limiting data collection and tracking will impact data-tracking companies and companies that have big stakes in ad networks like Google, Yahoo, Apple, Adobe, Facebook,

Microsoft, etc. However, these companies have resources at their disposal to allow them to move swiftly to adapt to the regulations.

In addition to regulations, many startups like Abine, Allow, Evidon and IntelliProtect are selling services to disable tracking. According to the Wall Street Journal, some of the giants (like Microsoft and McAfee) are already hedging their bets. Some online-tracking companies themselves are rolling out new ways to protect users from having their movements monitored online. AOL, one of largest online trackers, recently increased promotion of their privacy services. enCircle Media, an ad agency that works with tracking companies, invested in a privacy start-up, IntelliProtect. Companies like Allow use European legislation make data scarce by removing customers from the marketing databases, and in turn, sell their data for willing customers in return for a portion of the fee received for the data.

Despite the many businesses involved, this will ultimately impact users. The Internet is a free, interactive medium. As the input is limited, there will be an obvious impact to user experience. While people will have greater control over privacy on one hand, they will lose the richness of the Internet experience. There is a need to balance privacy with ensuring Internet growth.

1.3 Summary of the Report

The Internet is a vital part of economic and social life, and federal data privacy legislation should ensure that beneficial uses of data are not curtailed by overly restrictive data sharing policies. In this report, we will explore some business options which can make the user feel safer about the collected data by the internet service provider and also monitor the behavior of the internet provider for wrongly-collected user information. We will analyze the existing and future companies that work on data privacy to make the Internet prosper as a free service, as well as ensure that customers enjoy greater privacy.

2. Government Regulations

2.1. USA Privacy Laws

The privacy policies of American companies are voluntary, with the exception of protection under federal laws for certain kinds of sensitive information like health records and data about children younger than 13. On December 1, 2010, the Federal Trade Commission (FTC) published a preliminary report highlighting consumers' right to prevent websites from tracking their online behaviors. The FTC set the standards for use of an online opt-out function that allows consumers to forbid the collection or use of private information, and to demand a business entity to comply with the choice of a consumer to opt-out of such collection or use. In 2011 and 2013, there were several bills introduced around this issue, which were then dropped after industry groups said they would voluntarily develop ways for users to opt out. However, the industry groups were unable to come to an agreement with consumer rights groups about how to create such mechanisms.

Industry groups argue that tracking is necessary because it helps advertisers show users pertinent ads, which pay for the sites. Furthermore, tracking is more or less anonymous: since data trackers follow IP addresses rather than users directly, no significant information about users is revealed.

Several Web browsers and tech companies have already given users Do Not Track options. Google built Do Not Track support into its Chrome Web browser in February 2012 and Yahoo implemented a Do Not Track service across its entire global network last March. Mozilla, Microsoft, and AOL have also committed to working with Do Not Track technology. However, without a law, companies are not required to comply with user wishes to opt out. Sen. Jay Rockefeller introduced the Do Not Track Online Act of 2013 again, allowing the FTC to go after those companies that aren't complying with the law. The FTC would also be required to create the mechanisms that would let users choose whether or not they want to be tracked.

2.2. European Union Privacy Laws

Europe has tougher data protection rules. European Union policy makers are proposing to harmonize new, tougher rules across the 27-member union. These would require companies to obtain permission before collecting personal data and specify exactly what information will be collected and how it will be used. If asked, companies would have to provide users with data that has been collected about them and allow them to fix inaccuracies. One proposal would include a so-called "right to be forgotten" [8] that would make it mandatory for companies like Facebook to delete all information about users who want to wipe their slate clean.

Overly costly and restrictive rules have impacted the competitiveness of Europe's digital companies. European companies are at a disadvantage compared to U.S. companies because the government is essentially limiting their revenue to less than half of what they could otherwise earn. As a result, Europe has struggled to be an effective player in the Internet economy, whereas the United States is under significantly fewer restrictions.

When Europe unveiled proposals last year to toughen up data protection rules, they were hailed as an important advance in privacy rights. Now Brussels is weighing whether or not to adapt some aspects of the draft regulations in response to concerns over the impact on business. They want to ensure these changes do not sacrifice the fundamental principle that individuals are the ultimate owners of their own personal data.

2.3 Drawback of "Do Not Track"

The latest Consumer Insights Survey reveals that 68 percent of the Internet population across 11 countries would select a "do not track" (DNT) feature if it were easily available. This would create a 'data black hole' in the Internet.

Industry claimed data collecting is used to enhance user experience, and to target advertising based on user activity. As regulation tightens, data collection could "diminish personal data supply lines and have a considerable impact on targeted advertising, CRM, big data analytics, and other digital industries" [3]. The survey found that only 14 percent of respondents believe Internet companies are honest about how they use consumers' personal data, suggesting that it will be a challenge for online companies to change consumers' perceptions.

2.4 Business Approach to Government Regulations

Online publishers and advertisers are wary of the new regulations. Many large businesses have a group of lawyers who dedicate most of their time to fighting privacy litigations and lobbying against stricter regulations.

Companies have also created their own privacy policies and get explicit user consent from the users by making it a prerequisite to being able to use their services. In addition, they allow users to view and manage the information collected by the service provider.

3. Privacy Landscape

3.1 Data Ecosystem

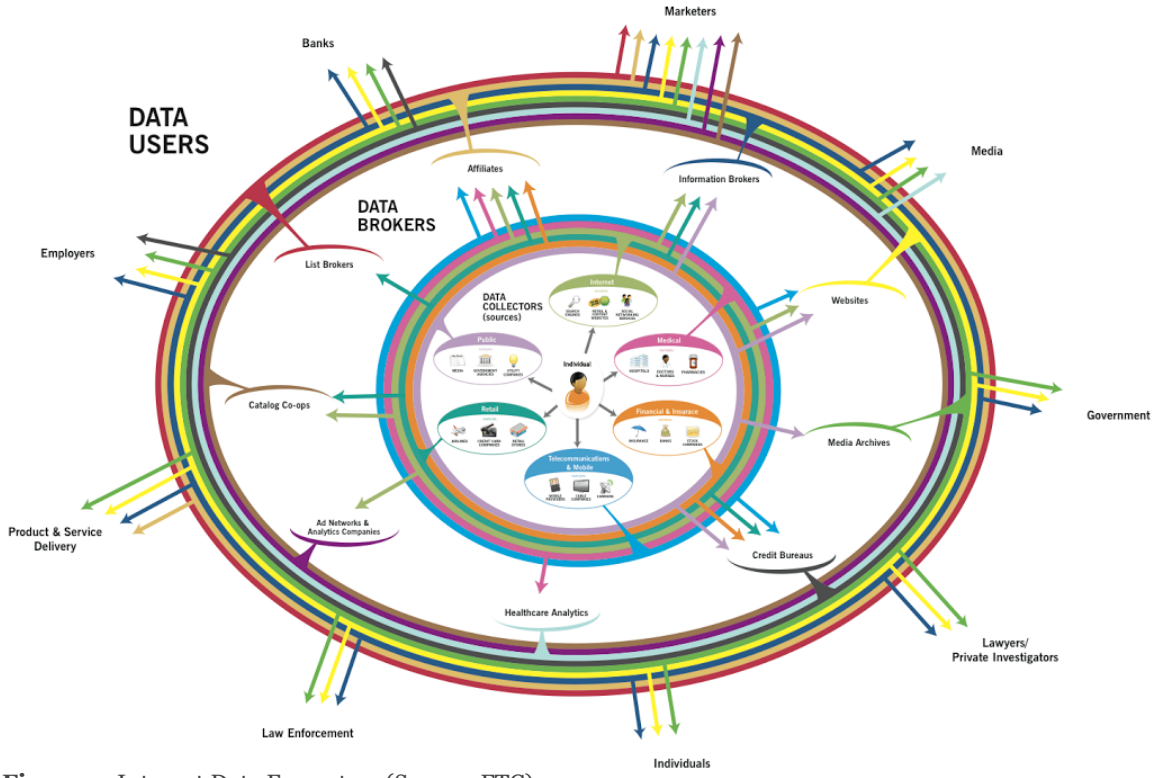


Figure 2: Internet Data Ecosystem (Source: FTC)

As we see from the above Federal Trade Commission (FTC) diagram [12], there is a large ecosystem around data. The User sits in the middle of the ecosystem. There are three main players:

- Data Collectors – Typically these are the players who are responsible for collecting the data from the users. Internet Websites are big Data Collectors from the users visiting their websites.
- Data Brokers – These players get Data from the Data Collectors, and analyze the data, generate some intelligence and make it available to Data Users. Credit Bureaus are Data Brokers who get data from different Data Collectors and make it available to banks for their business.
- Data Users – These players buy data from the Data Brokers and use this information in their business.

3.2 Technology Landscape

The advent of the HTTP cookie in 1994 enabled data collectors to profile users. A cookie is a special piece of information, usually opaque, that servers can send down to users' browsers. The browser then sends that information back to the server on subsequent accesses. By generating a unique cookie that identifies a user, the servers can now track users' behavior. Many cookies are persistent and survive multiple browser restarts and computer reboots. This enables the server to identify the user even if the accesses are weeks apart.

Many Web advertising companies attach cookies to their ad imprints (often pictures). This enables the advertising companies to track users' browsing behavior across multiple sites on which the ad company imprints their advertisement. This form of cookie usage is viewed as problematic, as tracking can occur without the knowledge of the data provider (the owner of the main content of the web page). It is also nearly impossible for users to recognize that a third party is tracking him or her.

Social network services take tracking to another level by using people's desire to connect with others online to entice them to disclose more information. Users' names, education, job history, place of birth, etc. are often public or accessible to the service provider irrespective of privacy settings. This reckless practice has raised controversy and fear among users. New technologies on the horizon can help the public take privacy into their own hands.

Proxy servers or anonymizers have been available since the early 90's. This technique routs users' web access to (untrusted) web services via one, often trusted, proxy server. To untrusted web servers, the access will appear as though it was originated from the proxy server, as it hides the IP address of the original user. Unfortunately, this technique does very little against cookies and web services that explicitly require users to log in (e.g. social networking sites.)

Data brokers' ability to analyze massive amount of raw tracking data has improved significantly in recent years, which has enabled them to produce more accurate and higher-value data. One obvious and expected reason for such change is the technology curve. Computers have been getting both faster and cheaper. More noteworthy is the advent of cloud computing and how it frees data brokers from making massive up-front capital investments. For example, instead of buying and managing 1000 computing nodes and allowing them to depreciate over 3 years, brokers can "rent" or buy the use of 2000 nodes for 1 year for the same price or maybe even rent 10,000 nodes for 1 month. This new service model is providing brokers with greater capabilities and flexibility to produce more valuable data.

As discussed above, the trend of technology and industry tends to favor data collectors, data brokers and data users, and makes it increasingly harder for online users to protect privacy and anonymity. However, due to increased user awareness and legislative pressure, a plethora of solutions looking to balance the needs of the businesses and consumers is emerging.

3.3 Industry Solutions

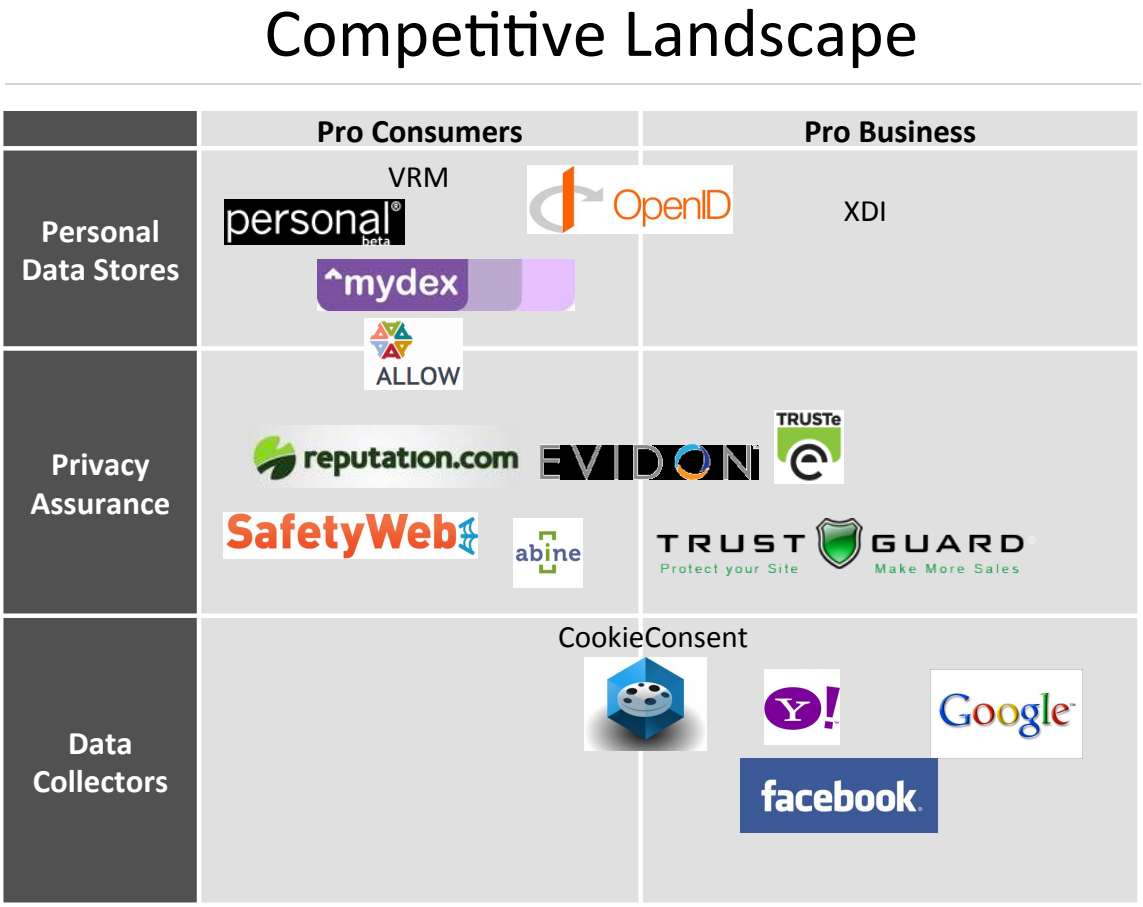


Figure 3: Competitive Landscape

Current players in the industry of data privacy solution providers can be categorized into following buckets:

1. Personal Data Store Solutions
2. Data Privacy Assurance Solutions
3. Data Privacy Scanning and Cleanup Solutions

3.3.1 Personal Data Store Solutions

Personal Data Store Solutions take an end-user-centric approach by enabling users to create "data vaults" and have control over what they share, and with whom. One example is MyDex (mydex.org). It allows users to manage, analyze and share personal data in a controlled manner. MyDex allows end-users to consume different services like Government Services, Energy Utility account and Telecom accounts *through* MyDex instead of directly consuming these services from the web. End-users will be attracted to MyDex primarily due to privacy concerns and the ability to "take control" over their personal data. MyDex makes money by charging various organizations to share the

personal data with them. Essentially, MyDex brings privacy-conscious end users to these services that might otherwise shun using them. However, this solution provides these services with presumably *higher quality* information of the specific end-users and provides a channel for directed marketing.

Evidon is on a mission to reveal the "invisible web" while promising privacy for the general public and high quality data analytics for Web publishers. It specialized in Global Tracking of various tracking technologies, and strikes at the intersection between the demands for advanced advertising technology and public awareness of privacy concerns. Evidon has a product called Ghostery that enables customers to take total control over what information is shared on the web.

3.3.2 Privacy Assurance Solutions

Companies like Trust-e and Trust Guard allows websites to gain credibility with its visitors. They verify the privacy and security policies of websites, audit them at regular intervals, and then provide a *seal of approval*. These companies also act as *watchdogs* by taking customer complaints and having the ability to take the trust seal away from companies. They also specialize in understanding government regulations and incorporate them into their assurance programs. Trust-E is the first organization to join US-EU Safe Harbor law, which is the de facto framework for companies to comply with US-EU data and privacy standards.

3.3.3 Scanning and Cleanup Solutions

While companies like MyDex and Evidon try to prevent users' private data from *leaking* online, *Data Privacy Scanning and Cleanup solutions, e.g. Reputation.COM* helps users when their data has already leaked and need to cleanup those records. These solutions scan the wide online world for reference to your private data and helps

1) Map out where a user's data is referenced
2) Update any discrepancy
3) Remove unwanted references to a user's data

4. Current Value Chains

In the series "What They Know" [7], the Wall Street Journal (WSJ) documented how the information economy of the Internet tracks people's behavior, activities, interests and data over several years, and how the privacy concerns associated with this. Below, we look at the value chains of this economy as described in the WSJ and how it is getting shaped and what opportunities arise from these trends.

Companies like Google, Facebook and Yahoo have spent billions of dollars to provide a long list of free services like blogs, news sites, search engines, email, and mapping tools that are largely taken for granted. These companies are counting on online advertising to fund and profit from these free

services. The following picture shows the ecosystem supporting the information economy – a web of tracking companies, data brokers, and advertising networks.

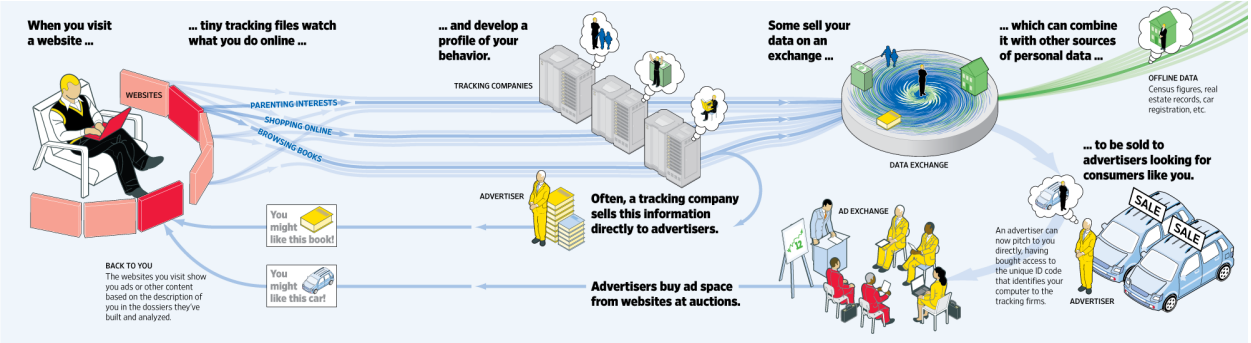
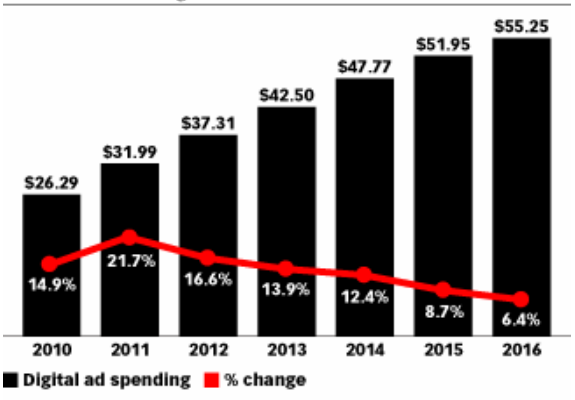


Figure 4: Ecosystem of the Internet economy (Source WSJ)

In the 90s, online advertising focused on websites with most visitor traffic. Over the last decade, that focus has shifted to personalized advertising. According to a study sponsored by the ad industry in 2009, the average cost of a targeted ad was $4.12 per thousand viewers versus $1.98 per thousand viewers for an untargeted ad. This potential revenue motivated advertising companies to start using tracking tools like cookies, flash cookies and beacons to collect data, mine data, and generate user profiles. Companies like Google, Microsoft, Adobe, and Apple not only have a big say in how much information can be collected about users, but also have big stakes in online advertising. Microsoft bought aQuantive for $6 billion, Google bought DoubleClick Inc for $3.1 billion, and Adobe bought Omniture for $1.8 billion.

eMarketer estimates that the digital ad spending market will increase to $55 billion by 2016 in the US alone [9].

US Digital Ad Spending, 2010-2016
billions and % change



Note: includes advertising that appears on desktop and laptop computers as well as mobile phones and tablets, and includes all the various formats of advertising on those platforms; data through 2011 is derived from IAB/PwC data
Source: eMarketer, Sep 2012; confirmed and republished, Dec 2012
144424 www.eMarketer.com

US Digital Ad Spending Share, by Format, 2010-2016
% of total and billions

	2010	2011	2012	2013	2014	2015	2016
Search	**45.7%**	**47.2%**	**47.1%**	**46.5%**	**45.5%**	**44.9%**	**44.2%**
Display	**37.7%**	**38.5%**	**40.2%**	**41.6%**	**43.3%**	**44.5%**	**45.6%**
—Banner ads	23.7%	23.6%	23.3%	22.6%	21.5%	20.9%	20.4%
—Video	5.4%	6.3%	7.9%	9.7%	12.0%	13.4%	14.5%
—Rich media	5.8%	5.2%	4.9%	4.8%	5.0%	5.2%	5.5%
—Sponsorships	2.7%	3.5%	4.2%	4.5%	4.8%	5.0%	5.2%
Classifieds and directories	**9.9%**	**8.1%**	**7.0%**	**6.4%**	**5.9%**	**5.5%**	**5.3%**
Lead generation	**5.1%**	**4.8%**	**4.6%**	**4.5%**	**4.4%**	**4.2%**	**4.0%**
Mobile messaging	**1.0%**	**0.8%**	**0.6%**	**0.5%**	**0.5%**	**0.4%**	**0.4%**
Email	**0.7%**	**0.7%**	**0.6%**	**0.5%**	**0.5%**	**0.5%**	**0.4%**
Total	**$26.29**	**$31.99**	**$37.31**	**$42.50**	**$47.77**	**$51.95**	**$55.25**

Note: includes advertising that appears on desktop and laptop computers as well as mobile phones and tablets on all formats mentioned; data through 2011 is derived from IAB/PwC data
Source: eMarketer, Sep 2012
144428 www.eMarketer.com

Figure 5: Internet Revenues (Source eMarketer)

With the advent of location awareness in mobile devices and increased usage of smart devices like smartphones and tablets, targeted advertising is going one step further. Now an ad can be sent to a consumer at the desired time, at the desired coordinates. Data is collected through not only online activities but through Apps downloaded and used on these smart devices. Google operates its AdMob and Apple runs its iAd network for the Android devices and Apple devices respectively.

5. New Opportunity

As companies begin to aggressively track consumers through online and mobile technologies, privacy advocates, consumers and governments have begun to engage in efforts to limit and control this activity. There is an obvious erosion or privacy and legitimate concerns about this user data falling into wrong hands – a situation very similar to that in the 1960s-70s in relation to credit agencies who had extensive information on customers and were willing to sell it to anybody [10]. The result of such invasion of privacy led to the eventual regulation of credit agencies through the 1970 Fair Credit Reporting Act [11], which allowed consumers to access and collect or remedy their information. Privacy and the information economy are going through a similar phase.

Privacy protection has become a commodity. A lot of startups selling monthly/annual services to "take control of your privacy" have emerged. These startups essentially monitor, disable tracking, mask users when accessing the Internet, delete personal information from websites, etc. Tightening regulations in Europe and a similar trend in the US and elsewhere also is moving to limit access to user data. These solutions have the potential to limit the rich Internet experience and its myriad and extensive uses.

In order to create a healthy and free Internet Services ecosystem, the following needs to happen:

- Government regulation should bar tracking with user identity, but allow the collection of consumer information for targeted service. This will require auditing web sites to ensure compliance.

- New privacy tools and messaging campaigns must be developed by publishers to convince consumers that they can be trusted. Improving the transparency of data collection and use will help to build trust, and that will increasingly become a sustainable competitive advantage.

There are substantial gaps in the current technologies and service offerings and cannot support this new environment. New services and additional/improved technologies are need in the following spaces to help create a healthy web services ecosystem:

1) As privacy regulations allow collection of consumer information without violating user privacy, it will become harder to ensure that all companies are complying with regulations. Ensuring compliance will require independent auditors, similar to those in the finance industry, to check the behavior of data collectors. The certification by the auditors will help companies prove they

are accountable to the government as well as end users, so that users can trust the web services providers and are more open to do business with them.

2) In the new environment, the companies will still comply with the five core principles of privacy: Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security, and Enforcement/Redress. Even though companies are addressing these principles individually, end users cannot access this information in a consistent and uniform way using a single standard taxonomy. Rather, there is an opportunity to make this information easily accessible to the end users across multiple publishers without (a) sharing information from one publisher to another and maintaining individual publishers' competitive advantage or (b) storing user information in a single place and becoming a target for hackers.

3) Additional security tools will also be necessary, as publisher websites will be audited more closely. They will need tools to detect and address vulnerabilities on their websites. There will be need for additional tools for the auditing and reporting. And last but not least, end users will need tools to protect their private data over and above that which is provided by #2.

5.1. New Ecosystem

The government will recognize these auditing companies, similar to its relationship with auditing companies in the finance industry. This will allow the government to create healthy regulations, which will help the Internet Industry grow without compromising the privacy of end users.

Independent auditors will keep service providers accountable to end users. This will allow end users to manage their information easily, privately and consistently.

Today's security solutions are designed to widen the gap between the consumers and web publishers, because they are either Pro-consumer or Pro-business. In the new ecosystem, tools would be designed to close the gap instead of increasing it.

5.2. Value Net

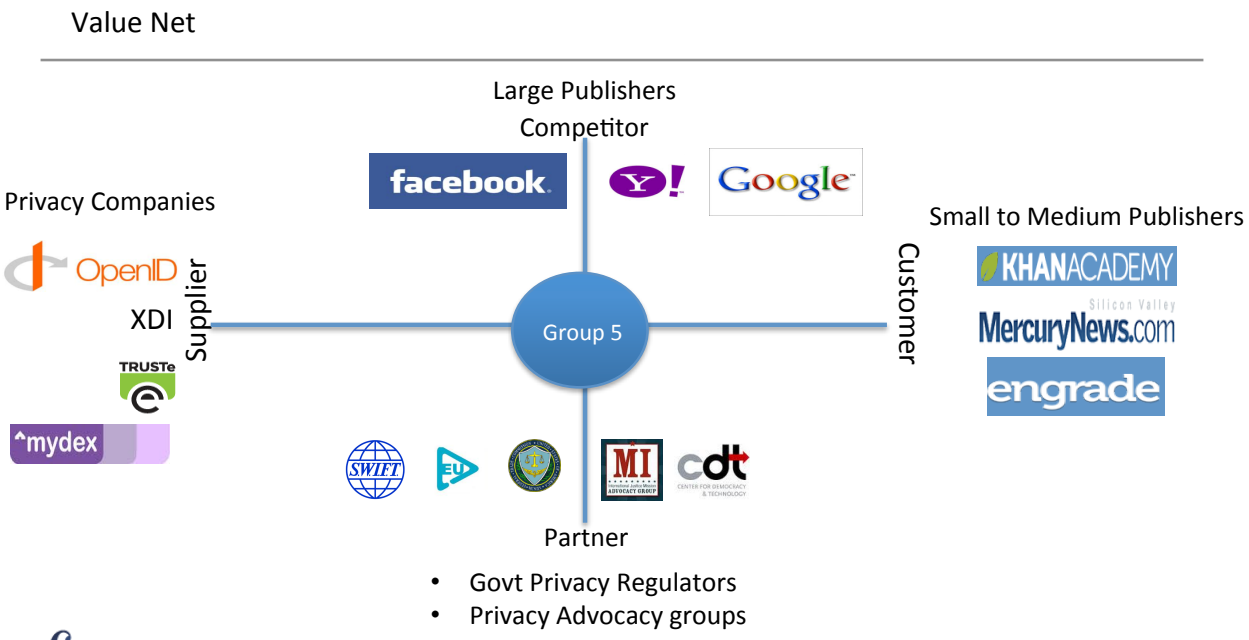


Figure 6: Value net of possible opportunities

Using this description, with our proposed opportunity in the center of the value chain, we see the following:

- Small and medium publishers will be the customers. They will benefit because they will be able to stay competitive without violating privacy regulations. Just as the finance industry uses internal auditors, these publishers will be able to stay compliant. With certification from external auditors, they will be able to prove compliance to the government and to end users.
- A strong partnership will be built with government privacy regulators. The government sees auditors as trusted partners who help created balanced regulations, and rely on the auditors to ensure publishers are compliant.
- Big publishers will not use this company's services in the beginning, probably because they believe they can successfully remain independent. They will lobby for privacy regulations on their own. However, we believe that big publishers will realize that lobbying is not core to their business and can be easily outsourced.

Companies that provide tools and services to enhance privacy will be the new suppliers. Their tools will help protect publisher websites, which will make it easier to audit and certify these companies.

6. Conclusion

Interest groups have long considered online privacy a priority. The actions that the government takes to enable Internet users to control the amount of data they share and how the share it will undoubtedly have a profound effect in the online data ecosystem. As identified in this report, the government must create balanced regulations and monitor publishers' compliance to these regulations. The end users need to feel more comfortable sharing their information online to enjoy a better user experience without compromising privacy.

In the Opportunities section, this report identified three areas in which there are significant gaps in the existing ecosystem. New services and solutions in these areas will help create a healthy ecosystem, without which the $9B Internet economy, growing at 18 percent, will be severely impacted. This is obvious from the comparison of the US and EU economies, where costly and restrictive rules have impacted the competitiveness of Europe's digital companies.

Biographies

1. Internet Advertising Revenues Hit Historic High in Q3 2012 [http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-121912]
2. The Value of Behavioral Targeting [http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf]
3. Stricter Privacy Regulations for Online Advertising Will Harm the Free Internet.
4. Net benefits:How to quantify the gains that the internet has brought to consumers; Economist March 9th, 2013
5. https://www.privacyrights.org/online-information-brokers-list , Mar 2013
6. (http://businesstoday.intoday.in/story/do-not-track-tools-could-choke-internet-economy/1/192141.html)
7. "The What They Know" series (http://online.wsj.com/public/page/what-they-know-digital-privacy.html), the Wall Street Journal (WSJ)
8. http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten
9. http://www.emarketer.com/newsroom/index.php/digital-ad-spending-top-37-billion-2012-market-consolidates/
10. http://en.wikipedia.org/wiki/Equifax.
11. 1970 Fair Credit Reporting Act (http://en.wikipedia.org/wiki/Fair_Credit_Reporting_Act
12. http://www.ftc.gov/bcp/workshops/privacyroundtables/personalDataEcosystem.pdf

Acknowledgement: This paper was created in an open classroom environment. There should be no proprietary information contained in this paper. No information placed in this paper is intended to affect or influence public relations of any firm affiliated with any of the authors.

FUNG INSTITUTE
for **ENGINEERING LEADERSHIP**

The Coleman Fung Institute for Engineering Leadership, launched in January 2010, prepares engineers and scientists – from students to seasoned professionals – with the multidisciplinary skills to lead enterprises of all scales, in industry, government and the nonprofit sector.

Headquartered in UC Berkeley's College of Engineering and built on the foundation laid by the College's Center for Entrepreneurship & Technology, the Fung Institute combines leadership coursework in technology innovation and management with intensive study in an area of industry specialization. This integrated knowledge cultivates leaders who can make insightful decisions with the confidence that comes from a synthesized understanding of technological, marketplace and operational implications.

Berkeley

National rankings consistently place UC Berkeley's undergraduate and graduate programs among the world's best. Berkeley is home to top scholars in every discipline, accomplished writers and musicians, star athletes, and stellar scientists—all drawn to this public university by its rich opportunities for groundbreaking research, innovative thinking and creativity, and service to society.