The future of online consumer protections

A Consumer Watchdog policy conference

Wednesday, Dec. 1
8 am – 3 pm
Washington, DC
# The Future of Online Consumer Protections: A Consumer Watchdog Policy Conference

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00 AM</td>
<td>Registration, Continental Breakfast</td>
</tr>
<tr>
<td>8:30 AM</td>
<td>Welcome from Consumer Watchdog’s Jamie Court and John M. Simpson</td>
</tr>
<tr>
<td>8:45 AM</td>
<td>Keynote speaker</td>
</tr>
<tr>
<td></td>
<td><strong>David Vladeck</strong>, Director, Bureau of Consumer Protection, Federal</td>
</tr>
<tr>
<td></td>
<td>Trade Commission</td>
</tr>
<tr>
<td>9:30 AM</td>
<td>Protecting consumers while they surf the Web: How “Do Not Track Me”</td>
</tr>
<tr>
<td></td>
<td>would work and other ideas</td>
</tr>
<tr>
<td></td>
<td><strong>Chris Soghoian</strong>, Privacy and security researcher</td>
</tr>
<tr>
<td></td>
<td><strong>Susan Grant</strong>, Director of Consumer Protection, Consumer Federation</td>
</tr>
<tr>
<td></td>
<td>of America</td>
</tr>
<tr>
<td></td>
<td><strong>Ginger McCall</strong>, Staff Counsel, EPIC</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Protecting electronic health records and ensuring patient safeguards</td>
</tr>
<tr>
<td></td>
<td>in the online medical marketing era</td>
</tr>
<tr>
<td></td>
<td><strong>Dr. Deborah Peel</strong>, Founder, Patient Privacy Rights</td>
</tr>
<tr>
<td></td>
<td><strong>Jeff Chester</strong>, Executive Director, Center for Digital Democracy</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Competition and antitrust issues on the Internet</td>
</tr>
<tr>
<td></td>
<td><strong>Gary Reback</strong>, Of Counsel, Carr &amp; Ferrell LLP</td>
</tr>
<tr>
<td></td>
<td><strong>Scott Cleland</strong>, President, Precursor LLC</td>
</tr>
<tr>
<td></td>
<td><strong>Melanie Sabo</strong>, Assistant Director for Anticompetitive Practices,</td>
</tr>
<tr>
<td></td>
<td>Bureau of Competition, Federal Trade Commission</td>
</tr>
<tr>
<td>12:30 PM</td>
<td>Lunch</td>
</tr>
<tr>
<td>1:00 PM</td>
<td>Luncheon Keynote</td>
</tr>
<tr>
<td></td>
<td><strong>Daniel J. Weitzner</strong>, Associate Administrator, National Telecommunications and Information Administration, Department of Commerce</td>
</tr>
<tr>
<td>2:00 PM</td>
<td>The Internet’s impact on creative arts</td>
</tr>
<tr>
<td></td>
<td><strong>Stuart Bernstein</strong>, literary agent</td>
</tr>
<tr>
<td></td>
<td><strong>Michael Capobianco</strong>, Science Fiction and Fantasy Writers of America (SFWA)</td>
</tr>
<tr>
<td></td>
<td><strong>Salley Shannon</strong>, American Society of Journalists and Authors</td>
</tr>
<tr>
<td></td>
<td>(ASJA)</td>
</tr>
<tr>
<td>2:50 PM</td>
<td>Wrap-up and adjourn</td>
</tr>
</tbody>
</table>
Table of Contents

Speaker Biographies

I. Protecting consumers while they surf the Web: How “Do Not Track Me” would work and other ideas


Common Sense Media poll on online privacy. October 8, 2010.

Christopher Soghoian, “End the charade: Regulators must protect users’ privacy by default.”


Consumer Federation of America, “Why We Need a “Do-Not-Track” Mechanism to Protect Consumers’ Online Privacy.”


II. Protecting electronic health records and ensuring patient safeguards in the online medical marketing era


Center for Digital Democracy, “‘Visit Two Websites and Tweet Me In The Morning’ Questions Consumers Should Ask About the Hidden Dangers of Online Health and Medical Marketing.”

III. Competition and antitrust issues on the Internet


Speaker Biographies

David C. Vladeck is the Director of the Federal Trade Commission’s Bureau of Consumer Protection. The Bureau works to protect consumers from unfair, deceptive, or fraudulent practices. The Bureau conducts investigations, sues companies and individuals who violate the law, promulgates rules to protect consumers, and educates consumers about their rights and responsibilities. The Bureau also collects complaints about consumer fraud and identity theft and makes them available to law enforcement agencies across the country.

Vladeck is on leave from Georgetown University Law Center, where he is a Professor of Law. Before joining the Georgetown faculty, Vladeck spent over 25 years with Public Citizen Litigation Group, handling complex litigation. He has argued a number of cases before the US Supreme Court and more than 60 cases before the federal courts of appeal and state courts of last resort. Vladeck testifies frequently before Congress and writes on administrative law, preemption, first amendment, and access to justice issues.

In May 2008, Legal Times of Washington recognized him as one of 30 “champions of justice,” and one of the 90 greatest lawyers in Washington, D.C., over the past 30 years. Vladeck is a graduate of New York University and Columbia law school.

Daniel J. Weitzner serves as Associate Administrator for Policy at the United States Commerce Department’s National Telecommunications and Information Administration (NTIA). NTIA is principal adviser to the President on telecommunications and information policy.

Prior to joining NTIA, Weitzner created the MIT CSAIL Decentralized Information Group, taught Internet public policy in the Electrical Engineering and Computer Science Department, and was Policy Director of the World Wide Web Consortium. He founded the Web Science Research Initiative with Tim Berners-Lee, Wendy Hall, Nigel Shadbolt and James Hendler. Weitzner was co-founder and Deputy Director of the Center for Democracy and Technology, and Deputy Policy Director of the Electronic Frontier Foundation.

Weitzner has a law degree from Buffalo Law School, and a B.A. in Philosophy from Swarthmore College. His writings have appeared in Science magazine, the Yale Law Review, Communications of the ACM, Computerworld, Wired Magazine and Social Research.

Susan Grant is Director of Consumer Protection at the Consumer Federation of America, a nonprofit association of some 300 nonprofit consumer groups that was established in 1968 to advance the consumer interest through research, education, and advocacy. Ms. Grant works specifically in the areas of privacy, deceptive marketing,
online safety and security, fraud, electronic and mobile commerce, and general consumer protection issues.

She coordinates CFA’s Fake Check Task Force, conducts CFA’s annual Consumer Complaint Survey, and is a recognized authority on combating consumer fraud and deception. She began her career in 1976 in the Consumer Protection Division in the Northwestern Massachusetts District Attorney's Office and has worked in the consumer protection field ever since.

Christopher Soghoian is a Graduate Fellow at the Center for Applied Cybersecurity Research at Indiana University. His research is focused on the intersection of applied computer security, privacy, law and policy. His work has resulted in the successful passage of an amendment to Indiana's data breach laws, a congressional investigation of web security flaws at the Transportation Security Administration, as well as several media firestorms, such as his December 2009 disclosure of evidence revealing that Sprint Nextel had provided its customers’ GPS information to law enforcement agencies over 8 million times in a single year.

Until August 2010, he was employed as the first ever technologist within the Division of Privacy and Identity Protection at the Federal Trade Commission.

Ginger McCall is Staff Counsel Assistant Director of EPIC's Open Government Project. Ms. McCall works on a variety of issues at EPIC, including consumer protection, open government requests, amicus curiae briefs, and national security matters. She litigates EPIC's Freedom of Information Act lawsuits and is a co-editor of Litigation Under the Federal Government Laws 2010. Ms. McCall has co-authored several amicus curiae briefs on privacy issues to the Supreme Court of the United States. She has been invited to speak on privacy and open government issues in a variety of academic and conference venues, including the 2009 Computers, Freedom, and Privacy Conference, the Internet Governance Forum USA 2009 Conference, and the New England Consortium of State Labor Relations Agencies 11th Annual Conference. Ms. McCall has also provided expert commentary for local, national, and international media, including NPR, MSNBC, and Al Jazeera.

Ms. McCall is a graduate of Cornell Law School and graduated magna cum laude from the University of Pittsburgh with a B.A. in English Literature. While in law school, she interned at the American Civil Liberties Union in Pittsburgh and at EPIC. Ms. McCall was the president of the Cornell Law School National Lawyers Guild and was awarded Cornell's Freeman Prize for Civil and Human Rights.

Deborah C. Peel, MD is a psychoanalyst and health privacy expert. She founded Patient Privacy Rights in 2004, now with 12,000 members. PPR is the nation’s leading consumer
watchdog for health privacy. PPR is the voice for Americans who want control over electronic health information to protect jobs, opportunities, and their children’s futures.

Dr. Peel also leads the bipartisan Coalition for Patient Privacy, representing 10.3 million Americans. Coalition principles form the core of the historic new consumer protections in ARRA/HITECH: a ban on the sales of PHI without consent, audit trails, segmentation, breach notice, the right to prevent disclosure of PHI for payment and HCO if payment is out-of-pocket, and encryption. She was elected one of ModernHealthcare’s “100 Most Powerful in Healthcare” from 2007-2009.

Jeff Chester has been an important force in public-interest media issues for more than twenty years. He is one of the nation's leading advocates working on telecommunications issues. In 1996, Newsweek magazine named him one of the Internet's fifty most influential people. His first book, *Digital Destiny: New Media and the Future of Democracy*, was released in January 2007. A former investigative reporter and filmmaker, he has long been at the forefront of the fight against consolidation and commercialization of the U.S. media system.

He received his MSW in Community Mental Health from UC Berkeley in 1978 and his BA in psychology from California State University, San Francisco in 1975.

Scott Cleland is President of Precursor, LLC, which consults for Fortune 500 clients; authors the "widely-read" PrecursorBlog.com; publishes GoogleMonitor.com and Googleopoly.net; and serves as Chairman of NetCompetition.org, a pro-competition e-forum supported by broadband interests.

Eight different Congressional subcommittees have sought Cleland's expert testimony on a wide range of complex emerging issues related to competition, and Institutional Investor twice ranked him as the top independent telecom analyst in the U.S. Cleland has been profiled in Fortune, National Journal, Barrons, WSJ's Smart Money, Investors Business Daily, and Washington Business Journal.

Gary Reback is a well-known antitrust lawyer. At one time or another, he has represented many of the most prominent Silicon Valley IT companies in antitrust and intellectual property cases.

Last year, Gary founded the Open Book Alliance to oppose the Google Book Settlement, currently pending in federal court in New York. OBA members include the New York Library Association and the Special Library Association (corporate libraries), various author groups and small publisher associations, and big high tech companies like Yahoo!, Amazon, and Microsoft.
Reback is of counsel in the Litigation Practice Group of Carr & Ferrell. He specializes in intellectual property and trade regulation litigation and counseling. He has represented many of Silicon Valley's best known companies in high profile litigation and transactions and has won many technology cases in the Federal trial and appellate courts around the country, including *Lotus v. Borland* in the United States Supreme Court.

Over the years, Mr. Reback has been named to the "100 Most Influential Lawyers in America" list by the *National Law Journal*, The "Elite 100" by *Upside Magazine*, the "Top 100" by *Micro Times*, and "Lawyers of the Year" by *California Lawyer Magazine*. He has been profiled in *The New Yorker*, *The New York Times*, *Wired Magazine*, *The Financial Times*, and *Business Week*, among other publications.

Perhaps best known for authoring the widely read "White Paper" successfully opposing Microsoft's acquisition of Intuit, Mr. Reback was counsel for the Anonymous Amici, opposing the Justice Department's first consent decree with Microsoft. He is generally credited with spearheading the efforts leading to the U.S. Government's prosecution of Microsoft.

Mr. Reback has written articles for *Forbes* and other business publications and is an advisor to a number of Silicon Valley start-up companies. He received his undergraduate degree from Yale University and his law degree from Stanford University.

**Melanie Sabo** joined the Federal Trade Commission's Bureau of Competition as Assistant Director of the Anticompetitive Practices Division in November 2007. Ms. Sabo previously was a partner in the Antitrust Law & Trade Regulation Practice Group at K&L Gates.

She has worked for the Antitrust Division of the United States Department of Justice, served as Counsel to the Antitrust Subcommittee of the Senate Judiciary Committee, and clerked for the Honorable William J. Castagna, United States District Court for the Middle District of Florida. Ms. Sabo also spent several years working as a Biomedical Engineer for Johnson & Johnson before attending law school.

**Stuart Bernstein** is an independent literary agent based in New York City. A former bookseller, he founded his agency, Stuart Bernstein Representation for Artists, in 1995, and works with writers of literary fiction and non-fiction in all categories. Bernstein has been an outspoken critic of the Google Books Settlement.

**Michael Capobianco** is the co-author, with William Barton, of four science fiction novels, and the sole author of one more. He served as President of Science Fiction and Fantasy Writers of America (SFWA) from 1996-1998 and 2007-2008. A long-time observer of the digital publishing scene, Capobianco acts as point man for SFWA on the Google Books Settlement.
**Salley Shannon** is a freelance writer and the current president of ASJA, the American Society of Journalists and Authors (ASJA), which represents the nation's independent, nonfiction writers, whether their work appears in books, magazines or online. She had been president for five weeks when she read the originally proposed version of the Google Book Search settlement one night after dinner, and became outraged at perceived violations of copyright and anti-trust law buried in its complex pages. She subsequently began rallying writers in opposition to the settlement. ASJA has twice lodged objections with the court, as has Shannon personally.

In more than 20 years as a freelance writer, Salley Shannon has always had assignments from major circulation magazines on her desk. She has written for Woman's Day, Reader's Digest, Parents, Good Housekeeping, Saveur, Smithsonian, More, and myriad other publications, including her hometown magazine, the Washingtonian. Now a generalist, she originally specialized in science and health care reporting. Her work has been nominated for National Magazine Awards in both the reporting and feature writing categories.

**Jamie Court**, President of Consumer Watchdog, is an award-winning and nationally recognized consumer advocate. His latest book, "The Progressive's Guide To Raising Hell: How To Win Grassroots Campaigns, Pass Ballot Box Laws And Get The Change You Voted For," was published by Chelsea Green in September 2010. "Americans angry about the state of their government or the fallout from the BP oil disaster might find in Court's persuasive manifesto a cause for action," Publishers Weekly writes. "With great accessibility and a fired-up attitude, Court brings his lessons in empowerment to the people."

Court is also the author of "Corporateering: How Corporate Power Steals Your Freedom And What You Can Do About It" (Tarcher Putnam, 2003) and co-author of "Making A Killing: HMOs and the Threat To Your Health" (Common Courage Press, 1999). The Los Angeles Times calls Court "a tireless consumer advocate." The Wall Street Journal writes, "He's notorious for his dramatic, sharp-tongued attacks on the health- and auto-insurance industries, and on any politician who takes their campaign cash." Court helped to pioneer the HMO patients' rights movement in the United States, sponsoring successful laws in California and aiding them elsewhere. He has also led major corporate campaigns to reform insurers, banks, oil companies, utilities and political practices. Court is a regular commentator on National Public Radio's "Marketplace" program and on the Los Angeles Times op-ed page.

Court has also worked as an advocate for the homeless and as a community organizer. He has a degree in history from Pomona College.
Carmen Balber is the director of Consumer Watchdog's Washington, D.C. office, and its eyes, ears and voice on national public policy. She is also point person for research and advocacy that exposes the corrupting influence of cash and corporation on politicians. She coordinates Consumer Watchdog's public education efforts on medical malpractice and is a legislative advocate on issues ranging from financial system and healthcare reform to protecting the civil justice system and corporate accountability.

Balber is a recognized political reform expert and a consistent critic of special interest political influence and attempts by politicians to skirt campaign and ethics laws. Her exposure of corporate funding for exotic overseas junkets have led to new rules on politicians' travel and luxury spending. Through media outreach, citizen organizing and public education, Balber ran the campaigns to pass the nation's strongest conflict of interest protection, the Oaks Project's Taxpayer Protection Acts, in five cities across California. Balber coordinated citizen organizing efforts in Consumer Watchdog's successful grassroots campaign to block a legislative utility bailout in 2001, including leading a three-week volunteer lobbying effort in Sacramento at the end of the 2001 legislative session.

Before joining the Oaks Project and Consumer Watchdog, Balber served as Assistant Canvass Director for the Colorado Public Interest Research Group (COPIRG). She holds a B.A. in Politics from Pomona College.

John M. Simpson, director of Consumer Watchdog’s Inside Google project, is a veteran journalist who held top editing positions at international, national and community newspapers. Most recently he was executive editor of Tribune Media Services International, a syndication company. He was previously deputy editor of USA Today and editor of its international edition.


Simpson holds a B.A. in philosophy from Harpur College of SUNY Binghamton and was a Gannett Fellow at the Center for Asian and Pacific Studies at the University of Hawaii. He has an M.A. in Communication Management from the University of Southern California's Annenberg School for Communication.
Protecting consumers while they surf the Web: How “Do Not Track Me” would work and other ideas
POPULAR Fixes on Issue of Internet Privacy, Tracking, & Children

Is it “important” to have “more laws that protect the privacy of your personal information?”

- **YES:** 90%
- **NO:** 10%

- **Important:** 23%
- **Very Important:** 67%

*Poll source: Consumer Watchdog / Grove Insight*
POPULAR FIXES ON ISSUE OF INTERNET PRIVACY, TRACKING, & CHILDREN

Require the creation of an “anonymous button” that allows individuals to stop anyone from tracking their online searches or purchases.

YES: 86%

NO: 9%

*Poll source: Consumer Watchdog / Grove Insight
POPULAR FIXES ON ISSUE OF INTERNET PRIVACY, TRACKING, & CHILDREN

Ban the collection of any personal data on children under the age of 18.

*Poll source: Consumer Watchdog / Grove Insight*
Prevent online companies from tracking personal information or web searches without your explicit, written approval.

*Poll source: Consumer Watchdog / Grove Insight
Ban the collection of any personal data on children under the age of 18.

Poll source: Consumer Watchdog / Grove Insight
Popular fixes on issue of Internet Privacy, Tracking, & Children

Require the creation of a “do not track me” list for online companies that would be administered by the Federal Trade Commission.

YES: 80%

NO: 12%

*Poll source: Consumer Watchdog / Grove Insight*
Support extending current advertising protections regarding children beyond TV, radio and print to online advertising.
TO: Interested Parties

FROM: Lisa Grove and Ben Patinkin
Grove Insight, Ltd.

RE: Findings from a Recent Poll on Internet Privacy and the Role of Congress

DATE: July 27, 2010

This analysis is based on a survey of 1000 likely 2010 general election voters. A base sample of 800 voters was conducted nationally and an oversample of 200 voters was conducted in California. This survey was conducted over the Internet with respondents pulled from a panel of previously identified voters. Interviews were conducted July 22 to 25, 2010 and the margin of error is +/- 3.1% at the 95% percent level of confidence.

Americans Are Concerned About Google’s Collection of Wireless Data.

While Google shows the strongest favorability ratings among the tech companies we tested (74% favorable, 8% unfavorable), our recent poll shows a significant majority of Americans are troubled about recent revelations that Google has been collecting wireless data information. Nearly two-thirds of voters nationwide (65%) say it is one of the things that “worries them most” or a “great deal” with

“Google has admitted that over the last three years it gathered communications from home WiFi networks without permission from the owner and stored the data on its servers.”

65% one of the things that “worries them most” or a “great deal”

“Google is cooperating with the federal government’s top electronic spy organizations, the National Security Agency or NSA, with no explanation of what information is shared.”

55% one of the things that “worries them most” or a “great deal”
another 20% saying it arouses “some concern.”

**Sharing Information with the NSA Also Raises Their Ire as They Call for Hearings**

A solid majority (55%) is also bothered (“one of the most” or “great deal”) by Google’s cooperation with the NSA without saying what information is being shared.

Even more voters call for Congressional hearings on “Google’s gathering data from home WiFi networks and its sharing of information with U.S. spy agencies like the National Security Administration, the NSA” (69% favor, 19% oppose).

Perhaps most importantly – at least for Members of Congress – voters appear to be in a punishing mood for those who refuse to hold hearings, especially if there are donations from Google in the campaign coffers. **Nearly six in 10 said they would be less likely to vote for their Member of Congress if they took campaign contributions from Google and then refused to hold hearings on the Wi-Spy scandal.**

Would you be more or less likely to vote for the Congressperson from your area if you found out they took campaign contributions from Google and then refused to hold hearings on the so-called “Wi-Spy” scandal perpetrated by Google, where the company gathered communications from home WiFi networks without permission from the owner and stored the data on its servers, or wouldn’t it make a difference to you either way?

More likely 12%
Less likely 59%
No different, not sure 29%

**Voters to Congress: Do Not Let Them Track Me and Do More to Protect Kids**

The public also shows deep support for a broad range of strong privacy protections. In fact, when asked whether it is “important” to have “more laws that protect the privacy of your personal information” nine in 10 (90%) support this notion. Of these, two thirds (67%) say it is “very important” and there are no real differences based on age—meaning voters under 50, including those ages 18-29 are just as likely to say more privacy laws are needed as those over the age of 70.

When asked specifically what laws they would like, attempts to block tracking are in strong demand. In fact, every proposal that included the word “tracking” receives support levels that were 70% or greater.

A “make me anonymous button” (86% favor, 9% oppose) tops the list, followed by preventing online companies from tracking personal information or web searches without your explicit, written approval (84% favor, 11% oppose).
Children should definitely be off limits according to these Americans. Cataloguing the online behavior of children in order to better advertise to young audiences is something 83% of Americans want banned. Banning the collection of any personal data on children under the age of 18 (84% favor, 10% oppose) is another proposal that is widely popular. There is also similar support for extending current advertising protections regarding children beyond TV, radio and print to online advertising (81% favor, 13% oppose)

### Popular Fixes on Issue of Internet Privacy, Tracking and Children

<table>
<thead>
<tr>
<th>Proposal</th>
<th>Favor</th>
<th>Oppose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require the creation of an &quot;anonymous button&quot; that allows individuals to stop anyone from tracking their online searches or purchases</td>
<td>86%</td>
<td>9%</td>
</tr>
<tr>
<td>Ban the collection of any personal data on children under the age of 18</td>
<td>84%</td>
<td>10%</td>
</tr>
<tr>
<td>Prevent online companies from tracking personal information or web searches without your explicit, written approval</td>
<td>84%</td>
<td>11%</td>
</tr>
<tr>
<td>Ban online companies from tracking and storing information related to children’s online behavior so they can target them with advertising</td>
<td>83%</td>
<td>12%</td>
</tr>
<tr>
<td>Require the creation of a “do not track me” list for online companies that would be administered by the Federal Trade Commission</td>
<td>80%</td>
<td>12%</td>
</tr>
</tbody>
</table>
Online Privacy: What Does It Mean to Parents and Kids?

Our kids’ mobile and online lives connect them to their friends and to the world. But even when kids believe that their information is protected, nothing is ever as private as they think. Anything kids post or text can get copied, pasted, forwarded, searched – and viewed – by unintended audiences, including teachers, college admissions officers, and marketers who want to capture your kids’ online information in order to sell to them. Sharing and social networks have benefits, but they also make our personal information very public.

Zogby International conducted a poll for Common Sense Media, asking both teens and parents about their views of online privacy and how they feel their personal information is being used by websites, social networks, and other online platforms.

Key findings

Parents are deeply concerned about how much kids are sharing.

- 92% of parents are concerned that children share too much information online.
- 85% of parents (and 83% of adults) say they are more concerned about online privacy than they were five years ago.
- Three quarters of parents (75%) don’t think social networking sites do a good job of protecting children’s online privacy.
- 91% of parents think search engines and social networking sites should not be able to share kids’ physical location with other companies until parents give authorization.
- Even teens (79%) think their friends share too much personal info online.

Families need clear and simple information about privacy.

- 51% of parents say they always/sometimes read Terms of Service (TOS).
- 91% of parents say they’d take more time to read TOS if they were shorter and clearer.
- 70% of parents (73% of adults) think schools should educate students about online privacy.

75% of teens think adults are a better source than their friends for advice on staying safe online.

Parents want changes from tech companies and leadership from government.

- 61% of parents want Congress to update online privacy laws for children and teens.
- Significant majorities – 88% of parents and 85% of teens – want online companies to get their opt in before the companies use their personal information for marketing.
- 69% of parents believe online privacy is a shared responsibility of individuals and online companies.
- 88% of parents would support a law requiring online companies to get their opt in.
What can we do to protect kids’ privacy online?

Protecting kids’ privacy online requires help from everyone. That’s why Common Sense Media has launched the Common Sense Privacy Campaign to help families defend kids’ personal information and reputations online. The campaign features specific ways that industry leaders, policymakers, parents, and educators can better protect our kids’ privacy online, including:

- Do not track kids – no behavioral marketing for kids.
- The standard for all kids’ privacy should be opt-in.
- Privacy statements should be clear and simple.
- Parents, teachers, and kids need to be educated about protecting privacy.
- Industry must innovate to protect kids and families.
- Government needs to update privacy policies for the 21st century.

The campaign includes tips and videos for parents, new privacy curriculum tools for teachers to use in the classroom, and comprehensive advocacy efforts to ensure that policymakers and online companies understand that in this 24/7 online and mobile world, where personal information is constantly bought and sold, parents need tools and information to help kids protect their privacy.

Common Sense Media has five simple privacy tips for parents:

1. **Make sure kids always use privacy settings.** They don’t want to be publicly searchable on Facebook or other social networks. And make sure kids understand that they can protect their privacy by “untagging” themselves in any photo.

2. **No location sharing!** When kids broadcast their whereabouts using sites like Gowalla, foursquare, or other location-sharing programs, it not only makes them vulnerable to unwelcome personal contact, but it also gives away personal information to advertisers.

3. **No questionnaires, free giveaways, or contests!** They scrape kids’ information and use it to market directly to them.

4. **Make sure kids look for the opt-out buttons.** When your kids register for a site or download an app, they accept the company’s use of private information. Make sure kids understand that many companies have “opt-out” policies – but they have to be proactive about checking those boxes.

5. **When in doubt, check it out.** Before letting your kid sign up for anything make sure you know the facts. New apps, ringtones, and features all come with baggage – do your homework on whatever the product is and who’s doing the selling.

To learn more about the Common Sense Privacy Campaign and to get involved, visit [www.commonsense.org/privacy](http://www.commonsense.org/privacy).

Common Sense Media is dedicated to improving the lives of kids and families by providing the trustworthy information, education, and independent voice they need to thrive in a world of media and technology. Through our education programs and policy efforts, Common Sense Media empowers parents, educators, and young people to become knowledgeable and responsible digital citizens.

For more information, go to: [www.commonsense.org](http://www.commonsense.org)

© 2010 [www.commonsense.org](http://www.commonsense.org)
End the charade: Regulators must protect users’ privacy by default

Christopher Soghoian
Center for Applied Cybersecurity Research, Indiana University
Draft of position paper for the Office of Privacy Commissioner of Canada

If you listen to executives from the online advertising industry, data aggregators, advertising supported webmail and social networking sites, consumers are extremely savvy. According to them, consumers know how to delete cookies,¹ and manage their browsers’ privacy settings to protect themselves from data leakage via referrer headers, CSS history stealing attacks and super cookies; they read through hundreds of advertising network privacy policies, and opt out of just those ad networks and data aggregators whose policies disclose problematic practices; they are aware of the risks associated with insecure (HTTP) web browsing when using public WiFi networks, and thus seek out and enable poorly documented SSL options in the services they regularly use; and of course, they customize their social network privacy settings, and don’t make any mistakes in the process.

This mythical tech-savvy consumer does not exist, even working within computer science departments, the offices of government privacy regulators, or the advertising firms themselves.

The vast majority of consumers do not understand cookies, have never heard of super cookies, referrer headers, or CSS history stealing, have likely never even tried to modify their browser’ privacy settings, have never read a privacy policy (and likely think that the mere presence of a privacy policy means that the site does a good job in protecting their data), have never opted out of a behavioral advertising network (and probably couldn’t name one, if asked), have no idea about the risks of checking their Facebook or Hotmail account at Starbucks, even after Firesheep.² Finally, if they have tried to customize their Facebook privacy settings, they probably made several mistakes in the process, and likely believe that their data is far better protected than it really is.

If the average consumer even knew about the numerous tools, browser add-ons and options to protect their privacy, many would be overwhelmed – however, most do not even know about these options, nor have they spent any time seeking them out, because they have no idea about most of the threats. When people think about privacy problems on Facebook – they think of their parents, ex-lover or employers seeing their private wall posts, not data brokers like Rapleaf building up dossiers to be sold for pennies to any interested buyer. Likewise, the only harm that most consumers reasonably expect at Starbucks is the obscene price of a latte, not the possibility that their email or social networking account can be hijacked by a hacker.

As one further data point, if executives at major websites like MSNBC, The Huffington Post, and Dictionary.com have no idea about the tracking cookies delivered via their own websites,³ how can we reasonably expect consumers to understand the practice?

¹ http://econsultancy.com/us/blog/5257-study-flash-cookies-are-not-the-answer-for-online-advertising
² See generally: http://codebutler.github.com/firesheep/
³ http://online.wsj.com/article/SB10001424052748703957804575602730678670278.html
It is time for government regulators to stop entertaining this charade of privacy policies that no one reads and opt-outs that no one uses. Consumers do not need to know how to change their oil to drive a car, and they should not need to know how to tweak obscure browser settings in order to safely browse the web. Regulators need to make sure that consumers receive comprehensive privacy protection, by default.

The key to doing this, I believe, is to transform the web browser into an effective privacy-enhancing technology. The web browser already controls the storage and transmission of cookies, supercookies and the transmission of referrer headers. Likewise, the browsers already include many configuration options and settings that, when correctly tweaked, significantly limit the degree to which consumers can be covertly tracked online.

Unfortunately, none of the browsers currently effectively protect privacy by default. One reason for this current state of affairs, at least for Chrome and Internet Explorer, is that these software products are created by online advertising networks, whose own profits would be hurt if users could not be tracked.

A Wall Street Journal exposé earlier this summer documented the internal deliberations over Internet Explorer's InPrivate Filtering feature, which, when enabled, blocks access to many third party servers, including behavioral advertising networks. As the Journal revealed, Microsoft's online advertising division was able to force the Internet Explorer team to disable this feature by default, and further require that users re-enable it each time the browser restarts. Because most users never change their software defaults, the effective impact of this decision was to expose millions of consumers to online tracking by behavioral advertising companies, including Microsoft's Atlas Solutions division, who would have otherwise have been protected had the feature been enabled by default.

Of course, Microsoft and Google could modify their web browsers to block all advertising networks other than their own. Such an action would prevent most forms of tracking, while still protecting the companies’ respective profit margins (and perhaps even increasing them, as advertising dollars would likely shift to their own networks). However, it is likely that such an action would raise significant antitrust issues – and so we are left with the present situation, in which consumers are exposed to silent tracking by hundreds of different ad networks.

In order to ensure that consumers are protected from various forms of online tracking, privacy regulators should compel the major browser vendors to modify their products. At a minimum, I recommend the following:

- Third parties should not be permitted to track users across different sites and over multiple browsing sessions. The browser vendors should either block both the setting and transmission of 3rd party cookies and supercookies by default, or should “double key” them.

4 “A further complication is that the three browsers referred above still transmit existing cookie information even when the browser settings are set to reject (new) 3rd party cookies. In other words, information about cookies which have been placed before setting the browser to reject cookies will continue being sent to the ad network provider. Only one major browser currently allows users to both block the setting and the transmission of 3rd party cookie data (i.e., including cookies placed before the setting of the browser to reject cookies). This has as consequence that also cookies that have been set as first-party (when visiting the single website of, for example, a search engine or a social networking site) can still be read by that site when the user visits a site that has partnered with that first website.” See: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp171_en.pdf at page 14.
to both the first and third party domains, such that they can no longer be used to track users across different first party sites.\footnote{See generally: https://wiki.mozilla.org/Thirdparty}

- Flash cookies, and Flash itself should no longer be given a free pass. Regulators should hold Adobe accountable for the poor privacy default of its widely used browser plugin. Third party sites should not be able to set any Flash cookies, and until Flash cookies can be controlled, examined and deleted by the browsers, all Flash cookies should expire after some reasonable period of time (as they currently last \textit{forever}).

- Referrer headers should no longer transmit the full URL of the page last viewed when a user connects to a third party site. Website owners have no legal right to know the search terms that draw visitors to their websites, and it is time to protect consumers from a practice in which the search engines are willingly, and proactively engaged. Chopping off everything after the “/” from third party referrer headers would both eliminate the leakage of search engine queries, and the sharing of online social network identifiers that have recently lead to major news stories, and lawsuits by class action firms.

- The browser vendors must follow Chrome’s lead, and embrace silent, auto-updates for security fixes.\footnote{See: “Why Silent Updates Boost Security” Thomas Duebendorfer, Stefan Frei, ETH Tech Report, vol. TIK 302 (2009). http://www.techzoom.net/papers/browser_silent_updates_2009.pdf} Consumers should not have to click on an annoying dialog (which they have been trained to ignore) in order to receive protection from security threats. All of the browser vendors, and popular software plugins like Adobe’s Flash and PDF Reader must embrace this model. Consumers cannot be protected from rogue advertising networks abusing browser privacy flaws unless they are running up to date software.\footnote{For an example of abuse of browser flaws by advertising companies, see: Dongseok Jang, Ranjit Jhala, Sorin Lerner, and Hovav Shacham. 2010. An empirical study of privacy-violating information flows in JavaScript web applications. In \textit{Proceedings of the 17th ACM conference on Computer and communications security} (CCS ’10). http://cseweb.ucsd.edu/~hovav/dist/history.pdf}

The behavioral advertising industry depends upon widespread consumer ignorance of the very practices in which these companies are engaged: Tracking users around the web, building up detailed dossiers on their browsing activities and combining them with profiles purchased from data brokers. For too long, these companies have taken advantage of consumers’ ignorance, and the sorry state of the privacy tools available to them. The best these firms have done is to offer up pathetic, poorly engineered opt-out mechanisms whenever the threat of regulation has appeared on the horizon, and embraced vague, loophole-riddled self regulatory frameworks that prohibit only the most heinous of practices.

Privacy by default will undoubtedly impact the advertising industry, and its ability to reach consumers. The industry has adapted to technical changes in the past, and it will certainly adjust to privacy-by-default. Regulators must put consumers’ privacy first, and ensure that the tools that consumers use to browse the web are keeping them safe, rather than intentionally facilitating covert online tracking.
“Thanks to Private Browsing, Safari doesn’t save or cache any personal information you enter or pages you visit. It’s as if you were never there.” [8]

“Firefox Private Browsing: Surf the Web without leaving a single trace.” [3]

Over the past few years, all of the major web browser vendors have embraced the concept of Privacy Enhancing Technologies (PETs), and added “private browsing” modes to their products. Publicly, the companies describe this feature as useful for consumers “shopping for a gift on a family PC” [14] or someone wishing to “to plan surprises like gifts or birthdays” [7].

The private browsing features are widely promoted, and have even been featured in TV advertising campaigns [12, 13]. Unfortunately, the browser vendors have adopted a very narrow threat model of attacks from which they will protect users. Private browsing modes primarily protect users from a local adversary, who sits down at a user’s computer, and attempts to look through their browsing history. Most importantly, the private browsing modes are not intended to effectively protect users from online tracking by third parties [4], from adversaries with access to or control over the user’s network connection, such as their ISP or employer, or from a motivated attacker (e.g. a suspicious spouse) willing to install spyware on their computer.

When a user initiates a private browsing session, each of the browsers display some form of text dialog to users. This text details the kinds of data, such as cookies and browsing history that are not retained when the feature is in use. Two browsers, Firefox and Chrome even go so far as to attempt to explain some of the limitations of their respective private browsing modes, and list the kinds of adversaries from which the user is not protected.3

Unfortunately, as with many browser warnings [15, 5], it seems pretty clear that consumers are ignoring this text, and therefore it is not possible for them to understand the limitations of private browsing mode. One example that illustrates that users are unaware of the limitations of private browsing comes directly from Mozilla. Despite the fact that “private browsing” does not protect employees from network surveillance conducted by their employers, Mozilla recently reported that the highest use of private browsing mode occurs between 11am and 2pm [17], during typical lunch break hours. Thus, it seems that employees are using the private browsing function included in the Firefox browser, expecting that it will keep the information they are transmitting over their employers networks from the surveillance conducted by their employers, even though Firefox warns users that this threat is specifically not covered.

To be clear, it is not that the private browsing mode features are broken – on the contrary, the browser vendors are for the most part delivering exactly what they claim to deliver. The problem is that consumers do not understand the many limitations of the private browsing mode. Furthermore, because most consumers do not fully understand many forms of online tracking or surveillance [11, 10, 16], offering a private browsing mode may give them a false sense of confidence and encourage them to engage in behaviors they would otherwise avoid (e.g., using a corporate network to view non-work related content during their lunch break).

The fact that consumers are ill equipped to understand the limitations of the private browsing modes makes the marketing of these privacy features highly problematic, since users are therefore likely to believe these features deliver far more actual privacy than they really do, simply based on the name of the feature. One solution to this might be to rename these features to more accurately describe what they actually deliver. Unfortunately, “protect yourself from mildly inquisitive local attackers who

3Google’s Chrome should be praised for having by far the clearest yet informative text which is displayed each time the user enters incognito mode.
aren’t motivated enough to install spyware on your computer mode” doesn’t exactly roll off the tongue.

A more comprehensive solution would be for the browser vendors to actually deliver the kind of privacy protections that many users reasonably expect that the private browsing modes already deliver. However, as I will now briefly argue, many of the browser vendors have a strong incentive to not ship effective, comprehensive privacy features in their products.

No incentive to deliver effective privacy enhancing technologies

Many of the browser vendors have worked very hard to earn the trust and support of IT departments, since many users are not often able to install software of their own choosing on their work or university supplied computer. As such, the browser vendors are loath to do anything to upset this relationship. For example, if a browser vendor opts to include technology in their respective browser that is specifically designed to allow users to evade monitoring software or web filters installed by schools and employers, the browser vendor will soon find their product removed from desktops by IT departments, and replaced with a competing browser that lacks such privacy enhancements.

Another incentive problem relates to the fact that the web browsers that consumers use are often made by advertising firms. That is, both Internet Explorer and Chrome, which make up the majority of the PC and smart-phone markets are made by online advertising companies (Google and Microsoft).

Earlier this year, the Wall Street Journal published an expose of the internal deliberations over Internet Explorer’s InPrivate Filtering feature, which, when enabled, blocks access to many third party servers, including behavioral advertising networks [18]. As the Journal revealed, Microsoft’s online advertising division was able to force the Internet Explorer team to change this feature to be disabled by default. Because most users never change their software defaults [9], the end result of this was to expose millions of consumers to online tracking by behavioral advertising companies, including Microsoft’s Atlas Solutions division, who would have otherwise have been protected had the feature been enabled by default.

As the Wall Street Journal’s expose so clearly demonstrated, some browser vendors may be unwilling to put users’ privacy first, if doing so will impact the profit margins of their advertising divisions.

4Mozilla is currently considering the possibility of offering an anonymous browsing mode, that would seek to protect users from a far more expansive list of privacy threats than the current private browsing mode [2].

Conclusion

As I have argued in this brief position paper, private browsing modes currently deliver little meaningful privacy to end users. Furthermore, the browser vendors are unlikely to build strong, privacy enhancing features into their browsers that enable considers to effectively protect themselves from online tracking by behavioral advertising networks, or network surveillance by employers and universities. Unfortunately, many users are likely to reasonably believe that “private browsing” modes deliver just that: privacy. Such users may put themselves at risk and engage in risky online behavior that they might otherwise not, if they fully understood the limitations of the browser vendors’ chosen threat model.

References


Why We Need a “Do-Not-Track” Mechanism to Protect Consumers’ Online Privacy

What is Online Behavioral Tracking and Targeting?
Consumers are being tracked on the Internet wherever they go, whatever they do, without their knowledge and consent. Information about their online activities – what they search for, what they click on, what they purchase, what they share with others – is compiled, analyzed, and used to profile them. Sometimes information that is gathered about them offline is added to create even richer profiles. This “behavioral tracking” is primarily used for marketing purposes at this point, but it can also be used to make assumptions about people in connection with employment, housing, insurance, and financial services; for purposes of lawsuits against individuals; and for government surveillance. There are no limits to what types of information can be collected, how long it can be retained, with whom it can be shared, or how it can be used. As the Wall Street Journal characterized it, “one of the fastest-growing businesses on the Internet is the business of spying on consumers.”

What do consumers think about online behavioral tracking and targeting?
Surveys clearly show that many consumers are uncomfortable with online behavioral tracking and targeting. For example, a 2009 survey by researchers at the University of Pennsylvania and the University of California found that 66 percent of respondents did not want the Web sites they visit to show them ads tailored to their interest, and when the common tracking methods were explained, an even higher number rejected tailored advertising. More recently, a poll commissioned by the nonprofit organization Consumer Watchdog in July 2010 revealed that 90 percent of Americans wanted more laws to protect privacy, 86 percent favored the creation of an “anonymous button” that allows individuals to stop anyone from tracking their online searches or purchases, and 80 percent wanted a “do-not-track-me” list for online companies that would be administered by the FTC.

Why are consumers concerned?
Some of the information that is tracked is sensitive, such as that related to people’s health conditions or sexual preferences. Another concern is that behavioral profiles created by online tracking can be used for purposes beyond simply deciding whether to display an ad for a pick-up truck or a sedan to a consumer – they can also be used to make assumptions about people for employment, insurance, housing or financial services. Decisions are even being made about consumers’ creditworthiness based on who their friends are on social networking sites! These assumptions may not be accurate – for instance, a person researching cancer online because of a friend’s illness might be wrongly assumed to have the disease. There are also concerns about access to online profiles by law enforcement agencies, lawyers in divorce proceedings and others who might use the information in ways that consumers would never expect. And some consumers may feel that it is simply unfair to follow them around the Internet when they are engaged in their own personal activities.
Don’t consumers already have protection from unwanted tracking?

No, there are no laws that require consumers to be given the choice of whether or not to be tracked, and voluntary programs offered by industry are not adequate. Not all companies that engage in behavioral tracking and targeting participate in those programs, and there are no real penalties for failing to comply with them. There are also many loopholes in industry programs; for example, they may not apply to tracking by or sharing profiles with a company’s many affiliates – other companies that are under the same corporate ownership but with which the consumer may not be familiar or have any relationship. Plus industry programs that enable consumers to choose not to be tracked are based on placing “cookies” on their computers. These electronic files are not always effective in stopping tracking depending on the methods that are used to do it, and they can be deleted.

How would a “Do-Not-Track” mechanism work?

A “Do-Not-Track” mechanism would not work the same way as the national “Do-Not-Call” registry with which many consumers are familiar. There would be no need to sign up anywhere or provide any personal information. It would be a setting in Web browsers (such as Internet Explorer) that consumers could use to indicate that they do not wish to be tracked. The browsers would express the consumers’ preferences to the Web sites they visit. It would be easy to implement and simple for both consumers and trackers to use. And just as consumers whose numbers are on the national “do-not-call” registry can opt-in to receiving calls from telemarketers on a company-by-company basis, so could consumers give permission for tracking by certain entities, in this case through their browser settings. All browsers would be required to include a “do-not-track” mechanism as a standard feature, at no extra cost to consumers. And just as important, all trackers would be required to honor the consumers’ preferences.

Where can I get more information?

For more information about the issues related to online behavioral tracking and targeting go to www.consumerfed.org/consumer-privacy/privacy and read the fact sheets, testimony and comments there. At http://donottrack.us, you will find helpful explanations of how a “Do-Not-Track” mechanism would work.
May 18, 2010

Julius Genachowski, Chairman
Federal Communications Commission
Room: 8-B201
445 12th Street SW
Washington, DC 20554

Dear Mr. Chairman,

We are writing to you regarding recent reports that Google intercepted and downloaded wireless access (Wi-Fi) communications as part of its “Street View” activity. We understand that Google also downloaded and recorded a unique device ID, the MAC address, for wireless access devices as well as the SSID assigned by users. As you may know, Representative Markey and Representative Barton, two senior members of the House Commerce Committee, wrote to FTC Chairman John Liebowitz to ask the FTC to undertake an investigation and to reply to certain questions by June 2, 2010.

We are writing now to bring this matter to the attention of the Federal Communications Commission and to urge you to open an investigation. EPIC has worked closely with the FCC in the past to establish privacy safeguards for users of communications services, having brought the issue of call records sales to the attention of the Commission in 2005, and having supported the subsequent rulemaking on the issue. EPIC also urged the Commission to investigate the improper release of Americans’ call detail information to the National Security Agency. More recently, EPIC filed an amicus brief in support of the Commission in its successful case to protect the privacy of consumer call record information.

---

We believe that the Commission should now turn its attention to the significant communications privacy issues arising from Google Street View.

Google launched the Street View service in May 2007, with "360 degree street level imagery" of five American cities.\(^4\) The service raised significant privacy concerns but those concerns focused exclusively on the images that the company was capturing and putting online by means of digital cameras affixed to its vehicles. Some people objected to the fact that the cameras went through residential neighborhoods and captured images through homes windows. Others were surprised to learn that their own images were posted on the Internet by Google.

Google defended the program from privacy objections by stating that they "have been careful to only collect images that anyone could see walking down a public street" and that they would "be sure to respect local laws."\(^5\) Almost a year after launch, after adding a number of locations, Google began blurring the faces of those who appeared in the pictures, citing privacy concerns but again making no mention of Wi-Fi scanning.\(^6\) Google also faced a federal court case that rose to the Third Circuit Court of Appeals, which ruled that the company could face liability for trespassing on private property.\(^7\) As the program has expanded to cover most of the United States as well as over 30 countries abroad,\(^8\) the company has begun capturing data not only with cars, but also with a large tricycle and a snowmobile.\(^9\)

But the reality of Street View was very different. Google has now admitted that Google Street View vehicles have been capturing communications data for years. Google never disclosed this activity. The fact of Google's Wi-Fi spying was obtained by Peter Schaar, the German Commissioner for Data Protection and Freedom of Information, who discovered that the vehicles were scanning networks to compile a database of networks and their physical locations for use in "location-

---


aware" advertising services. Schaar demanded a full audit of the data Google was collecting and the immediate removal of the scanners from the cars.\(^\text{10}\)

As part of the audit, it was revealed that not only was Google mapping the physical locations of the networks, but that the vehicles were capturing payload data, meaning all data flowing on those networks. Whatever Internet traffic that was taking place on a given network as the Street View vehicle drove past was captured and stored by Google.\(^\text{11}\)

None of Google's Wi-Fi activity was made known to the public or presumably to the Commission until the recent investigation undertaken by European privacy officials. In fact, Google still makes no mention of the Wi-Fi data collection activity on the web page specifically devoted to privacy concerns related to Street View.\(^\text{12}\)

This is extraordinary. The capture of Wi-Fi data in this manner by Google Street View could easily constitute a violation of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also known as the Wiretap Act, as amended by the Electronic Communications Privacy Act (ECPA) of 1986 to include electronic communications.\(^\text{13}\) Courts most often define "interception" under ECPA as "acquisitions contemporaneous with transmission."\(^\text{14}\) The Wiretap Act provides for civil liability and criminal penalties against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any ... electronic communication [except as provided in the statute]."\(^\text{15}\) The Wiretap Act imposes identical liability on any person who "intentionally discloses ... to any other person the contents of any ... electronic communication, knowing or having reason to know that the information was obtained through the interception of a[n] ... electronic communication in violation of this subsection," or "intentionally uses ... the contents of any ... electronic communication, knowing or having reason to know that the information was obtained through the interception of a[n] ... electronic communication in violation of this subsection."\(^\text{16}\) The Wiretap Act also states, "a person or entity providing an

\(^{14}\) United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002); Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994).
\(^{15}\) 18 U.S.C. § 2511(1)(a).
\(^{16}\) 18 U.S.C. § 2511(1)(c)-(d).
electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."17

The Wiretap Act provides for six exceptions from Section 2511(1)-(3) liability. The first five exceptions are clearly inapplicable, including such behavior as execution of FISA warrants and FCC enforcement actions.18 The sixth exception provides allowances for “electronic communication[s] made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.”19 In interpreting this provision, courts have only found communications systems to be so configured when access is common and easy, such as visiting a web site20 or accessing a shared iTunes library.21 In the closest analogue to Google’s behavior, one court ruled that using a police scanner to intercept unscrambled cordless telephone calls violated the statute.22 By intercepting and recording unencrypted Wi-Fi transmissions, it is very likely that Google violated the federal Wiretap Act.

The Commission is charged with protecting the interest of US consumers of communications services in the United States and with safeguarding the security and integrity of network services. Section 222 of the Communications Act, for example, sets out clear obligations for providers of communications services to safeguard the privacy of customer information. Section 705 of the Communications Act adds to the Federal Wiretap Act additional restrictions on the intercept of communication “by wire or radio” without authorization.23 Specifically, the Act states,

No person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any

19 Id.
information therein contained) for his own benefit or for the benefit of another not entitled thereto.\textsuperscript{24}

Violations of Section 705 carry strict penalties, with willful violations “for purposes of direct or indirect commercial advantage or private financial gain” meriting fines of up to $50,000 and prison for up to two years for a first offense.\textsuperscript{25}

Google CEO Eric Schmidt was recently quoted as saying, “no harm, no foul.”\textsuperscript{26} Of course, it is not necessary to show “harm” to prove an unlawful intercept. It is the intercept itself that is the violation. This is particularly important when the representation about harm is made by the party that engaged in the illegal activity.

To be sure, many people take advantage of open wireless access points to go online. Absent any criminal intent or conduct, we are not suggesting that that activity is unlawful. But Google’s conduct with Street View was very different. The company routinely and secretly downloaded user communications data and the company routinely and secretly mapped private communications hotspots. Moreover, they said not a word about the Wi-Fi data collection during the three-year privacy debate over Street View.

This is why the FCC must undertake an investigation. The FCC has broad authority to execute and enforce the provisions of the Communications Act\textsuperscript{27} and the Commission plays a critical role in safeguarding the privacy of American users of communications services.

We look forward to hearing from you as soon as possible regarding the action the FCC intends to take.

Sincerely,

Marc Rotenberg
Executive Director
Electronic Privacy Information Center (EPIC)

\textsuperscript{24} Id.
\textsuperscript{25} 47 U.S.C. § 605(e)(2)
\textsuperscript{27} 47 U.S.C. §151.
May 17, 2010

The Hon. Jon Leibowitz
Chairman
Federal Trade Commission
600 Pennsylvania Ave.
Washington, DC
20580

Dear Chairman Leibowitz,

I am writing to ask the Federal Trade Commission to investigate Google Inc.’s “WiSpy” debacle, in which the Internet giant’s Street View cars snooped for years on home Wifi networks and gathered private communications data sent over them.

Less than a month ago Google was publicly asserting that it did not collect private WiFi “payload” data. Last Friday Google changed course. It abruptly claimed it had made a “mistake” and hadn’t realized its Street View cars were snooping on private WiFi networks all along.

Google has demonstrated a history of pushing the envelope and then apologizing when its overreach is discovered. Given its recent record of privacy abuses, there is absolutely no reason to trust anything the Internet giant claims about its data collection policies.

We call on the Federal Trade Commission to document what data Google has been gathering, for how long and what the company has done with it. Google’s suggestion for a third-party audit is inadequate. That would be like getting to pick and pay the referees in a championship basketball game.

The Commission has the authority and public trust necessary to get to the bottom of Google’s dubious data collection practices and reveal exactly how consumers’ privacy has been compromised and what remedies are required. The Commission must determine what Google knew and when Google knew it. We urge you to launch an investigation immediately.

Sincerely,

John M. Simpson
Consumer Advocate

Cc: Commissioner Julie Brill; Commissioner William E. Kovacic, Commissioner J. Thomas Rosch; Commissioner Edith Ramirez; David Vladeck, Director Bureau of Consumer Protection
Protecting electronic health records and ensuring patient safeguards in the online medical marketing era
The Case for Informed Consent
August 2010

Why it is Critical to Honor What Patients Expect—
for Health Care, Health IT and Privacy.

On July 8th, 2010, HHS Secretary Sebelius announced
a new “Administration-wide commitment to make sure no
one has access to your personal information unless
you want them to.”

"A patient-centered health care system would be one
where medical records would belong to patients. Clinicians,
rather than patients would need to have permission to
gain access to them.”

Deborah C. Peel, MD
Founder

Patient Privacy Rights
www.patientprivacyrights.org
P.O. Box 248
Austin, Texas 78746
(512) 732-0033

With the assistance of:

Ashley Katz deJong

With acknowledgement and appreciation for assistance on legal issues to:

James C. Pyles
Powers, Pyles, Sutter & Verville, P.C.
1501 M Street, NW
Washington, D.C.
Overview

For centuries, patients have come to physicians seeking help. They reveal embarrassing symptoms and share unsettling fears and concerns, because they trust clinicians to keep their information private.

Today, patients still think doctors protect their privacy. In their most vulnerable states, patients trust that health professionals, hospitals, and medical facilities will respect their privacy.

And yet, as we move forward with electronic health records (EHRs), health information exchanges, and innumerable health databases, keeping records private becomes more and more difficult. **Personal health information is being used and shared in ways patients never imagined.**

A patient shares personal health information in order to receive treatment. However, once these details are shared to receive treatment, that personal information is used in many other ways, passed on and shared with other strangers in companies and government agencies that have no direct relationship with the patient; this is “secondary use” of personal health information.

Patients have not been told about secondary uses of their health information. Patients have not given consent for the secondary uses of their health information. This practice violates patient trust and the right to health privacy.

The monetary value of personal health information is staggering. The health information technology (health IT) industry has estimated annual revenues of $8-9 billion dollars/year. The annual revenue of the stealth health data mining and data sales industry is likely two to ten times more. Examples are not easy to uncover, but the estimate for just one small electronic health record (EHR) company with revenues of $100 million dollars/year from software sales is that it could earn $250 million dollars/year more by selling patient data.¹

Tremendous good can be achieved using health IT, but we must first face and deal with misuse and harm from the systemic practice of data mining and data theft.

Protecting privacy is not just a moral or ethical necessity, but a practical one. Billions of dollars have been allocated in the American Recovery and Reinvestment Act to establish an EHR for every American. **If patients cannot control personal information stored in EHRs, they will not trust health IT systems or data exchanges and will avoid them.**

A black market for totally private treatment will develop for those who can pay to protect themselves and their families from discrimination and reputational harm. If patients refuse to adopt and use EHRs because they cannot control who can see and use the data, it will be a tremendous waste of taxpayer dollars and our investment in health technology.

The powerful healthcare, health IT, and data mining industries are extremely resistant to changing existing primitive, privacy-destructive systems. As a result, patients have been forced to use health IT systems that allow others to decide when to use and disclose their sensitive records. Arguments are made that patient control over data is too technically difficult, too expensive, or too complex to build and require. Often industry executives argue that patients don’t know what they want, or that patients simply don’t understand health care.

Patient Privacy Rights strongly disagrees. Robust privacy-enhancing technologies are in use now that ensure both progress and privacy. Technology can lower costs by enabling individual control over protected health information (PHI) today. Using consent will simplify data exchange by eliminating the need for complex and expensive data-sharing agreements between “stakeholders” such as covered entities, business associates, and other secondary and tertiary businesses and corporations. Moreover, patients know what they want and expect their right to health information privacy.

It is a mistake to design health IT in a paternalistic manner -- assuming a corporation, vendor, provider or government agency knows what is best for each individual patient. Instead, we should build ‘patient-centric’ health IT systems. In the words of Don Berwick, MD, Administrator of the Centers for Medicare and Medicaid Services (CMS), we should build systems that ensure
“medical records belong to patients. Clinicians, rather than patients would need to have permission to gain access to them”.2

Today, the majority of providers, insurers and major corporations fail to offer even basic electronic consent tools. Policy makers and industry have set the privacy bar too low. Today, health care and health IT industries are not complying with existing state and federal privacy laws or our ethical rights to health information privacy.

We can do much better.

This paper considers the foundation of privacy and medical ethics. Next we outline key findings that demonstrate the public’s expectations for medical privacy. We address key arguments against patient control over personal health information. Finally, we conclude by offering technical, process, and policy solutions and recommendations for moving health IT forward with patient control.

Privacy is a long-established individual right. The public clearly expects that this right be recognized and accommodated in standards and policies. Privacy is not a new concept, but the foundation of trust in the physician-patient relationship. The federal government must require industry to build in patient control as an integral part of the foundation of all HIT systems as they are developed.

2 Donald M. Berwick, What ‘Patient-Centered’ Should Mean: Confessions of An Extremist, Health Affairs 28, no.4 (2009): w555-w565 (published online May 19, 2009)
Privacy: An Ancient Tradition, Protected on Many Levels

The right to keep health information private is reflected in the Hippocratic Oath dating from 5th Century B.C. This Oath is still taken by graduates of American medical schools. It is a core ethical principle reflected in the standards of professional ethics of all health professions. Patients expect that what they say in the doctor’s office will stay in the doctor’s office.

There is a clear national consensus for the right to health information privacy. The consensus developed in state laws, federal law, common and tort law, Constitutional law, and the ethical codes of all the health professions over the course of our nation’s history. Federal courts have found consistently that the right to informational privacy, as distinct from the right to decisional privacy, is protected by the Fourth, Fifth and Fourteenth Amendments to the United States Constitution. In fact, the constitutionally protected right to privacy of highly personal information is so well established that no reasonable person could be unaware of it.

Ten states have a right to privacy expressly recognized in their state constitutions. A physician-patient privilege is recognized in the laws of 43 states and the District of Columbia. A psychotherapist-patient privilege is recognized in the laws of all 50 states and the District of Columbia and has been recognized by the Supreme Court as a matter of federal common law. The HITECH Act signed into law in February of 2009 expressly recognizes such privileges and provides that nothing in the Act is intended to constitute a waiver. All 50 states and the District of Columbia recognize in tort law a common law or statutory right to privacy of personal information.

Americans Care Deeply About Their Privacy

What exactly does privacy mean? The right to privacy is generally defined as the right of the individual to control who sees their health information. Without the ability to control the use and disclosure of health information, the individual has no right to health information privacy. In other words, privacy means control over personal information. Without control, we have no privacy. The National Committee on Vital and Health Statistics defined privacy as “an individual’s right to

---

4 Whalen v. Roe, 97 S. Ct. 869, 877 (1977); Ferguson v. City of Charleston, 121 S. Ct. 1281, 1288 (2001). (“The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.”); U.S. v. Scott, 424 F.3d 888 (9th Cir. 2005); Douglas v. Dodds, 419 F.3d 1097 (10th Cir. 2005)
5 Sterling v. Borough of Minersville, 232 F.3d 190, 198 (3rd Cir. 2000)
6 The State of Health Privacy, Health Privacy Project (2000)
8 HITECH Act, section 13421(c).
9 HHS finding 65 Fed. Reg. at 82,464
10 HHS finding 65 Fed. Reg. at 82,465; Letter from National Committee on Vital and Health Statistics to HHS Secretary Leavitt, p. 2 (June 22, 2006).
control the acquisition, uses, or disclosures of his or her identifiable health data”. 11 As long as health care-related corporations and government agencies control the use and disclosure of our health information, we have no way to keep our information private.

A final report recently released from the federal Agency for Healthcare Research and Quality (AHRQ) describes findings from twenty focus groups held across the country. The focus groups were designed to elicit and understand consumers’ awareness, beliefs and fears concerning health IT. Further, AHRQ wanted to learn how consumers may wish to be engaged with health IT12.

The findings solidly confirm Americans’ desire to control their personal health information. Americans are generally supportive of health IT, but they want to be well informed about the consequences of disclosures and have the ability to restrict access and use of their information.

- A majority want to “own” their health data and to decide what goes into and who has access to their medical records.
- There was near universal agreement in all focus groups that if medical data are stored electronically, health care consumers should have some say in how those data are shared and used.
- A majority believes their medical data is “no one else’s business” and should not be shared without their permission.
- This belief was expressed not necessarily because they want to prevent some specific use of data but as a matter of principle.
- Participants overwhelmingly want to be able to communicate directly with their providers with respect to how their PHI (protected health information) is handled, including with whom it may be shared and for what purposes.
- Most believe they should automatically be granted the right to correct misinformation.

---

11 NCVHS June 2006, Report to HHS Sec. Leavitt, on “Privacy and Confidentiality in the Nationwide Health Information Network”.
Americans Will Go “Off the Grid” to Ensure Privacy

The California Healthcare Foundation found that 13-17% of consumers engage in information-hiding in the current system. **One in eight** Americans puts their health at risk *because of privacy concerns.* These individuals take the following actions:

- Avoid seeing their regular doctor,
- Ask their doctor to alter a diagnosis,
- Pay for a test out-of-pocket,
- Avoid tests.\(^{13}\)

Millions of Americans will opt-out of and/or block new systems that take away their control of sensitive records. A survey by the California Healthcare Foundation in 2010 found that sixty-eight percent of Americans are concerned about the privacy of medical records.\(^{14}\) Because privacy concerns are not addressed in today’s electronic health systems, real harm occurs now. Patients avoid care, suffer needlessly, and die.

- **HHS** estimated that **586,000** Americans did not seek earlier cancer treatment due to privacy concerns.\(^{[1]}\)
- **HHS** estimated that **2,000,000** Americans did not seek treatment for mental illness due to privacy concerns.\(^{[2]}\)
- **Millions** of young Americans suffering from sexually transmitted diseases do not seek treatment due to privacy concerns.\(^{[3]}\)
- The Rand Corporation found that **150,000** soldiers suffering from PTSD do not seek treatment because of privacy concerns.\(^{[4]}\)
- The lack of privacy contributes to the highest rate of suicide among active duty soldiers in 30 years.

\(^{1}\) 65 Fed. Reg. at 82,779
\(^{2}\) 65 Fed. Reg. at 82,777
\(^{3}\) 65 Fed. Reg. at 82,778

\(^{13}\) California HealthCare Foundation, Consumer Health Privacy Survey, (June 2005)  

\(^{14}\) California HealthCare Foundation, National Consumer Survey on HIT, (January, 2010)  
We Do Not Have a Transparent, Patient-Controlled Health Care System

A key problem in our current system is a false sense of the security and privacy of electronic health systems. In large part this is caused by misinformation about what the Health Insurance Portability & Accountability Act (HIPAA) Privacy Rule really says. The HIPAA Privacy Rule as originally written during the Clinton Administration required patient consent before any information could be shared:

2001

“...a covered health care provider must obtain the individual’s consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations.”
65 Fed. Reg. 82,462

During the Bush Administration, the Department of Health and Human Services (HHS) made changes to the HIPAA Privacy Rule that remain in effect today. Most importantly, the right of consent was eliminated. Healthcare-related businesses are no longer required to ask our consent for countless uses of personal health information. Consent is no longer required before health-related corporations or government agencies can use our records for “treatment, payment and healthcare operations.”

2002

“The consent provisions...are replaced with a new provision...that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations.”
67 Fed. Reg. 53,183

Over 4 million “Covered Entities” and millions more “Business Associates” still have broad permission to use all protected health information; neither patient consent nor advance notice are required. The terms ‘Covered Entities’ and “Business Associates” include providers, employers, government agencies, insurance companies, billing firms, pharmacy benefits managers, pharmaceutical companies, collection agencies, marketing firms and data miners.

It could be argued that most patients provide ‘implied’ consent or grant explicit permission for their information to be used for treatment and claims payment. But patients are not aware that their health data is used for “healthcare operations” purposes. This data-use category is extremely broad and subject to abuse.
Here is the definition of healthcare operations from the Code of Federal Regulations (CFR):

Health Care Operations, 45 CFR 164.506:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

   (i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
   (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
   (iii) Resolution of internal grievances;
   (iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
   (v) Consistent with the applicable requirements of §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Patient consent is no longer required before widespread sharing or disclosures of electronic health records. No matter how embarrassing or intensely personal the contents may be, our information can be shared. Your doctor may wish to protect your information, but once the records leave his/her office, he/she cannot control how the recipient uses your information.

According to Professor Latanya Sweeney, the secondary use of Americans’ personal health information in electronic health systems today is “unbounded, widespread,
hidden, and difficult to trace.”

Without the power to control personal health information, patient trust is difficult, if not impossible, to achieve and maintain. Most patients expect their doctors to do the ‘right thing’ by keeping their records private. Few patients are aware that as soon as health information leaves a provider’s office, the misuse and sale of this very personal information by unknown third parties increases exponentially. Surveys show that individuals have a “common belief” and “strong expectation” that their personal health information will not be disclosed without their consent.

It is gratifying to see that HHS is moving to meet consumers’ expectations and to restore the right of informed consent by changing flawed privacy policies. On July 8, 2010, HHS Secretary Sebelius announced an “Administration-wide commitment to make sure no one has access to your personal information unless you want them to.”

Dr. David Blumenthal, the National Coordinator for Health Information Technology, joined her at the press conference to state that “we want to make sure it is possible for patients to have maximal control over PHI (protected health information).”

Our position is that privacy is a long-established individual right. The public clearly expects healthcare providers, the health care system, and health technology vendors to recognize and accommodate this right in standards and policies. Privacy is not a new concept, but the foundation of trust in the physician-patient relationship. The federal government must require industry to build in patient control as an integral part of the foundation of all HIT systems as they are developed.

**De-identification and Data Anonymization are not Enough**

Some argue that de-identification or stripping names (anonymization) from data ensures that PHI cannot be re-identified; and therefore, data can safely be used for a myriad of purposes with no need to inform patients or obtain their permission. Industry claims that de-identified or anonymized data cannot be re-identified are unproven; no external audits or proof that de-identification or anonymization actually work are required or offered. There is no requirement to release the algorithms/methods used to enable experts to verify the methods of de-identification or anonymization.

Furthermore, techniques to re-identify data are improving daily. They are used commercially and for government surveillance (Fusion Centers). The reason these techniques are used is personal health information is far more valuable than other kinds of personal information. Professor Latanya Sweeney of Carnegie Mellon and Harvard, has proven that 87% of the population can be re-identified with just

---


gender, month or year of birth and zip code. **Data is either useful or anonymous, but never both.** Data may seem to be anonymous but when electronically cross-matched with other sets of public or proprietary data, the merged data sets can reveal identity.

---

**All Personal or Protected Health Information (PHI) is “Sensitive”.**

This issue of what health data is “sensitive” and whether patients can protect what they consider to be sensitive data from use and disclosure is much broader than an individual's desire to keep his/her sexual history, use of anti-depressants, or genetic test results private. In today's digital information age, the health data mining industry knits together rich, comprehensive profiles of every individual's health status. These profiles include data from traditional sources like health records systems, along with non-traditional sources including data from reward cards and grocery and pharmacy purchase cards. Health data miners use online searches, social networks, and public and private websites to continuously flesh out and update profiles of personal health data. They acquire or buy information from the many corporations that obtain our records without consent. These profiles are treasure troves of sensitive personal information that can be used for many harmful purposes, for health financial scores, to harm reputations, and for job and credit discrimination.

---

18 Paul, Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" VER. 0.99 SSRN: 8/14/2009
Truly, PHI is no longer “safe” or “protected” anywhere. The techniques for collecting, aggregating, and matching PHI from disparate sources are very sophisticated. Most Americans have no idea how much personal health information is collected about them online and from the healthcare system. For example, even “normal” blood test results collected as “baseline information” are critical information; they can be used in the future as proof health status has changed.

**Americans Do Not Support Giving Researchers a ‘Free Pass’**

According to a national survey commissioned by the Institute of Medicine (IOM) in 2008, only one percent of Americans would allow researchers free and open access to their health information without permission. The survey found that over 4/5 of the population opposes having their information used without their permission EVEN IF it is de-identified and the research was approved by an Institutional Review Board. However, eighty-seven percent are supportive of research, as long as they are asked and have control.¹⁹

Despite Americans’ overwhelming rejection of open access to the nation’s electronic health records, most of the health care industry and the IOM propose eliminating informed consent for research using electronic health records. Writing about the IOM’s recommendation, Mark Rothstein remarked:

> “Clinicians, researchers, and their institutions do not have the moral authority to override the wishes of autonomous agents. Individuals seeking treatment at a medical facility are not expressly or impliedly waiving their right to be informed before their health information and biological specimens are used for research. The recommendation of the IOM Report would automatically convert all patients into research subjects without their knowledge or consent.”²⁰

**There is No Longer a Need for a One-Size-Fits-All Privacy Policy**

Industry and government calls to create a new, one-size-fits-all national privacy policy are contrary to the longstanding rights and expectations of the nation’s citizens. The only privacy policy that everyone can agree with is that each person should be able to set his/her own policies.

In fact, AHRQ's Report found no support for the establishment of general rules that apply to all health care consumers. Citizen participants thought that they, as health care consumers, should be able to exert control over their personal health information **individually, rather than collectively.**²¹ A very large proportion of

---


²¹ AHRQ, p. 29
participants felt that they should be asked for their consent before their information was stored in an electronic system”22.

### AHRQ Sample of Feedback

- On the consent forms you could have lines and then check boxes.
- I authorize this, this, and this, maybe not this.
- You could have a consent form, but certain conditions could change...They would come to you and say, "Beyond this, if this situation occurs while I am with you...?" Then you could opt to expand the information to other people.
- Researchers should not have access to your medical files unless you give consent. Even if somebody is tapping into my record just for training, I’d still have a problem. Unless they asked you “if you agree or not agree” to have that done. And if I say “yeah, go ahead and do it.”
- I think that there should be a list of every single entity that could possibly access your medical records. And then you would check off the ones you would allow.

### Health CARE Should Focus on Patient Needs

Don Berwick, MD, also wrote eloquently about the importance of keeping patients at the center of their own health care and health information. In a 2009 Health Affairs article, he argued that an ideal practice is one whose patients would say “They give me exactly the help I need and want exactly when I need and want it.” [emphasis added].23

In the debate over health IT and its potential benefits, those who seek health care are rarely at the table. What patients want from electronic health systems ranks dead last. Industry, government, providers, insurers, third parties and technology vendors get what they want and need first, before patients. We would be wise to heed Dr. Berwick’s call:

“I suggest that we should without equivocation make patient-centeredness a primary quality dimension all its own, even when it does not contribute to the technical safety and effectiveness of care.” [emphasis added]24

---

22 AHRQ Publication No. 09-0081-EF
23 Berwick, w558
24 Ibid, w559

Page 13 of 21
Dr. Berwick’s definition of “patient-centered care” is:

The experience (to the extent the informed, individual patient desires it) of transparency, individualization, recognition, respect, dignity and choice in all matters, without exception, related to one’s person, circumstances and relationships in health care.

Dr. Berwick’s definition reflects exactly what Americans want. **Health IT must enable patient autonomy and choice if it is to be successful.** The primary goal of policy makers, regulators, health IT vendors and other stakeholders should be to honor patient consent decisions and to build health IT systems that enable patients’ directives to control data use and disclosure, unless otherwise required by law. Privacy protections must be comprehensive and meaningful to ensure trust and protect personal health information throughout the healthcare system and online throughout cyberspace.

**Arguments Against Consent**

Some argue that relying on patient consent will result in patients signing the same kind of blanket, advance, coerced ‘consents’ that have long been used to grant broad access to paper medical records. We agree that blanket “consents” are both harmful and illegal, because it is impossible to give informed consent to disclose information that will be created in the future.

**Blanket Consents**

There are two key ways to prevent blanket, advance consents from being used. First, enforce existing laws. Enforce the HIPAA requirement that anyone, including insurers, ask only for the ‘minimum necessary’ information needed for a specific purpose. For example, a patient should not be asked to disclose his/her entire record of a consultation visit or disclose his/her full chart to an insurer for claims to be paid. Insurers do not need entire records to pay claims. Those who seek access to PHI should obtain meaningful informed consent from the patient. Informed consents should be direct “one-to-one” consents, with a specific purpose and time frame. Those who are granted access should be clearly named or described.

Second, require the use of existing and newly developed technologies that enhance privacy and consent. In the future, all consents will be electronic. Consent tools can offer simple check boxes and systems that empower patients to ‘slice and dice’ exactly what data they share with whom. **Electronic consent technologies make it remarkably easier and far cheaper to do the following:**
- Contact individuals in real time for consent, eliminating the need for advance, blanket consents;
- Change and update preferences instantly online;
- Segment sensitive information (i.e., keep separate from routine information);
- Set broad directives for some uses and be contacted for any exceptions; and
- Automatically grant permission to access or receive updates to trusted doctors or others;
- Eliminate the use of Institutional Review Boards (IRBs) and Privacy Boards for granting access to thousands of patients’ electronic medical records for research. Patients can be automatically contacted by cell phone or email easily and cheaply.

The use of privacy-enhancing technologies will eliminate the need for broad, blanket consents. **Fortunately, decision makers can now require “patient-centric” health systems to be built using innovative consent technologies.** We can use advanced technologies to protect our privacy rights and meet patients’ needs. Health IT that protects privacy will assure public trust.

Recently at the Consumer Choices Technology Hearing in Washington, DC, seven privacy-enhancing technologies were demonstrated and discussed. The hearing is now available on video and the testimony of the technology developers and users is available online.  

Because the technology is available today, policy makers can require providers and health data exchanges to use modern electronic consent tools; these systems will improve patient engagement and trust, and enable providers to easily comply with existing laws and medical ethics. For example, providers could be prohibited from receiving Federal Medicare or Medicaid payments or any stimulus dollars if they do not use effective, robust electronic consent systems. Providers should be required to use systems that ensure patients control personal health information.

**Relying on Consent is Too Burdensome for Patients**

Some argue that patients are not capable of making informed decisions about the use of their health records and will feel burdened by having to give consent. But obtaining patient consent was the standard of practice in the United States before 2002 when the right of consent was eliminated by the Bush Administration.  

Since then, state and federal government and industry have added more policies and standards that limit patients' rights to control the use and disclosure of PHI.

Yet these policies have never been publicly debated. The status quo, where PHI is used freely without patient knowledge or consent, shocks and angers average Americans. Government and the health care industry should not assume that

---


26 HHS finding 65 Fed. Reg. at 82,474.
patients cannot understand or manage their electronic health information. Further, deciding that patients do not deserve the autonomy to choose who can see and use their PHI violates the right to privacy and our fundamental national principles.

Quality health care can only take place in trusted relationships. Providers, covered entities, and business associates that want access to PHI should build direct relationships with patients if they wish to use sensitive records. They should make time for education and have conversations with patients about the real risks and benefits of disclosing health information.

Dr. Berwick recommends that providers and researchers take on the “burden of giving real meaning to the phrase ‘a fully informed patient’ including a “mature dialogue.” If over time patients make unwise decisions, he recommends that “we should seek to improve our messages, instructions, educational processes and dialogue to understand and seek to remedy the mismatch.” We have the right to health privacy and expect all individuals, organizations, government officials, or corporations seeking access to our personal information to ask before using our PHI. *If you cannot explain in a clear, understandable manner why you need or want my health information, you cannot use or have it.*

**Solutions & Recommendations**

The only legal, ethical, and practical way to get a complete and accurate picture of Americans’ health and health data is to require those who want to use health data to ask permission first. Asking first is the only way to create trusted electronic systems. Paradoxically, patients will be willing to collect and share far more information with health professionals, knowing they control who can see and use it. Trusted systems based on informed consent will create the richest, most complete, and most accurate data for research. The better the data, the greater the potential benefits—both societal and personal—that we can reap from health IT.

If we substitute ‘consent’ decisions made by IRBs and Privacy Boards, whose interests often conflict with patients’ rights and expectations, for patient consent, the result will be less data and less reliable data. Alternatively, using information from records that fully-informed patients have checked for accuracy will improve the accuracy of research. Trusted researchers will obtain richer, more accurate, and more complete data. The integrity, detail, and reliability of information obtained with patient consent is far superior to and more complete than data obtained without informed consent.

**Restore Privacy in the Privacy Rule**

Clearly, Americans believe they should be in control of their personal health information. But few consumers are aware of the vast number of corporations and government agencies that use personal health information without their

---

27 Ibid, w561
permission. The right of consent must be restored to the HIPAA Privacy Rule. The blanket authority granted to millions of covered entities and business associates to use our PHI without consent for purposes of “treatment, payment and health care operations” must be eliminated. None of those uses of data should occur without explicit patient permission.

**Examples of Electronic Consent Systems Demonstrated at the Consumer Choices Technology Hearing**

Health IT can enable privacy and patient control. A number of examples that are in effect today were recently demonstrated for policy makers. These are just a handful of solutions that show control is not overly technical, complex or expensive.

Behavioral treatment and substance abuse treatment centers, that are members of the National Data Information Infrastructure Consortium (NDIIC), have been using an open source EHR for over 9 years. This open source EHR provides granular, electronic, informed consent. These EHRs are used in 9 states and regions, covering 22 jurisdictions. Additional states are implementing NDIIC systems. Large and small provider organizations, across large and small states and counties have generated and exchanged over 4 million clinical records point-to-point. Records are only disclosed with informed consent.

A “point and click” format allows clinicians to quickly and easily enter the patient’s specific consent directives. This makes it easy to know what information is released to whom, for what purpose, and for how long. Recipients cannot receive data unless they agree to use it only for the specific purpose requested. They must agree to obtain a new informed consent for other uses. This consent module is being translated into HL7 computer language for wide-spread use; the set of consent functionalities/choices in the NDIIC consent modules should be the minimum functionalities required for our health information in all IT systems and websites that handle PHI.

Another solution is HIPAAT's consent management tools that work with any EHR. HIPAAT allows patients to create very simple or detailed consent directives. Any or all of the following are parameters that may be selected: Consent type, purpose of use, who may or may not access PHI, and PHI granularity including all PHI, PHI within a given time period, PHI related to a specific medical condition, or specific PHI types (e.g. prescription history).

**Private Access** has created technology that allows each person to grant “private access” to all or selected parts of their confidential personal information. The individual makes a decision based on his/her particular needs and interests. It empowers patients to participate in research that matters to them and can be used

---

for consent in clinical settings and on websites. For example, one Private Access product, “Privacy Layer”, is an automated system that responds within seconds at a cost of less than a nickel. The answer to a researcher’s query for health records takes into account both applicable law and the potential research subject’s wishes. Pfizer has partnered with Private Access to use the technology to recruit subjects for clinical trials, based on the privacy directives of the potential research subjects. This Private Access product solves the most important research problem of all: how to do genetic research via trusted health IT systems and enable consumers’ choices to be respected. This consent system costs about $5/year per patient.

e-MDs’ EHRs enable physicians to segment patients’ sensitive data so that it is not disclosed. The records sent can either be ‘flagged’ as having some data elements missing or simply sent with empty data fields. e-MDs’ EHR has received the highest ratings from the American College of Physicians and the American Academy of Family Practice. And it complies with laws in all 50 states that require the segmentation of sensitive data and separate consent for its release. This system could be easily adapted to allow patients to choose which data is segmented. Every system that handles PHI must be improved to meet the laws in EVERY state that require the ability for patients to segment many kinds of sensitive data. e-MDs proves that the capacity for segmentation can be built into all EHRs.

Tolven Institute’s open source personal health record system (PHR) is being deployed in the Netherlands, where only patients can disclose their data, unlike the U.S. In the Netherlands, data can be disclosed and shared only from PHRs with patient consent. Once a patient consents to having a PHR, no further consent is needed since all importing and exporting of information in and out of the PHR occur because of the patient’s explicit actions. Doctors, hospitals, labs, pharmacies, etc are never allowed to share or disclose health information in the Netherlands; only patients can share their electronic medical records.

The Department of Veterans Affairs demonstrated open source consent technology available at no cost. It enables patients to decide what information they do or do not want to share, under which circumstances they wish to share, and with whom. Patient choices are captured in an electronic consent directive that assures that any restrictions patients place on disclosing their PHI are applied to their data at all times health information is exchanged. This consent technology is fully interoperable; it is capable of sharing the patients’ choices and directives with other healthcare organizations. The technology is scalable, standards-based, and can be used without replacing or changing existing legacy EHR systems. The system is being piloted in San Diego, where records will be shared with patient consent between the VA and Kaiser Permanente. When fully operational, the entire population of six million US veterans will be served.

InterSystems Corporation’s HealthShare Consent Framework was designed to enable patient consent to share data via Health Information Exchanges (HIEs) and over the Nationwide Health Information Network (NHIN). This software was built
to work with InterSystems’ “Cache” health data bases. Cache data bases are used by 67 to 85% of healthcare-related entities in the US. For example, the VA and EPIC EHRs both use Cache data bases. To date, only opt-out consent is offered by HealthShare Consent Frameworks. “Opt-out” consent means that all our data will automatically be shared with the HIE or via the NHIN unless we object and opt-out of HIEs or the NHIN completely before our data is disclosed, i.e., it is not possible to keep any sensitive health information from being widely disclosed. Patients are forced to allow access to everything in order to have the benefits of health IT. The “opt-out” consent approach violates our rights to selectively share health information. This deceptive way to force consumers into sharing data is used now in New York and Indiana, and proposed in many more states. According to InterSystems, their consent frameworks could offer robust consumer consent filters; patients could segment sensitive data by data type or class of information, date range of events, by the selection of certain users, and hide the presence of information at any location or facility.

The four HIEs now using HealthShare were not willing to offer patients any choice but opting-out of all data sharing. These four communities decided to severely limit how patients can configure their consent policies; they did not take note of patients’ expectations, existing legal rights, and medical ethics. The good news is that the 67-85% of the American healthcare system based on Cache health data bases can support patient consent choices and directives. Technology can be improved within all HealthShare Consent Frameworks to ensure that patient privacy expectations are met; the systems can be programmed to make it happen. The bad news is that many other HIEs across the nation may also decide to offer only deceptive, unfair opt-out electronic consents.

Privacy Profiles
One way to help people learn how to use electronic consent systems is to create ‘privacy profiles’, i.e., sets of consent ‘rules’ or directives individuals can choose from. This approach offers examples of how consent directives can be set up, so patients are not overwhelmed with too many choices or too much information. If a person ranks their privacy concerns very high, they might select Patient Privacy Rights’ ‘privacy profile’ as the default settings for consent, to ensure his/her directives are highly protective. Another person might trust the American Cancer Society and use their consent recommendations. Still another may choose a ‘middle-of-the-road’ ‘privacy profile’. Private Access has developed a number of ‘privacy profiles’ using real people’s consent directives as examples. Those who share their ‘privacy profiles’ explain why they made their choices to help others think about how to set consent preferences.

Health Record Banks
Health record banks or trusts are the simplest and best solution to the challenge of storing and enabling the exchange of data. A health record bank can make exchanges inexpensively while fully protecting privacy via patient control.
In the health record bank model, everything is done only with consumer consent. Consumers control their complete records in the health bank and they decide who gets to see which parts of their records. This protects privacy (since each consumer customizes their privacy policy), promotes trust, and ensures stakeholder cooperation since all holders of medical information must provide us with copies of all our health information when we request it. Patients control access to the complete copy of their records, and they can add information (such as diet, exercise, alternative therapies, occupational and environmental factors, etc). Of course, the source of each item of information is clearly marked. This enables accurate copies of official medical records to be clearly distinguishable from consumer entries.

Washington State, Louisville, KY, Kansas City, MO, and Ocala, FL are currently building Health Record Banks. Each health record bank (HRB) is a community or state-based health data repository that houses copies of complete health records that are controlled by patients. Whenever a patient receives care, records generated are deposited in his/her health record bank account. Non-profit community organizations provide governance and may contract with for-profit corporations to develop and operate the HRB.

In addition, health banks can enable participation in research without disclosing any data to researchers. Research queries can be run on all the health data of patients who consent to have their data used for a particular research study. The health bank would then return the query results to the researchers. This system minimizes the number of disclosures of PHI. Because every disclosure of PHI exponentially increases the risk of data theft, data loss, and exposure, being able to permit beneficial uses of personal health information without risking personal harm is critically important. ‘Distributed’ data systems or networked approaches where personal data is searched in every location are complex, costly, and make protecting privacy much more difficult. In addition, ‘distributed’ data systems create a major threat to data security, since our data will only as be secure as the ‘weakest link’.

**Conclusion**

Fortunately, innovative privacy-enhancing technologies enable patients to control personal health information, except in rare instances where disclosure is required by law. Further, they allow the patient to direct or restrict data flow from EHRs, electronic health systems, and databases with personal health information. Consumer control over PHI is the simplest, easiest, cheapest, fastest, and most efficient enabler of health information exchange. Consumers’ rights to control PHI by giving or withholding informed consent has the added advantage of complying with state and federal privacy laws, legal and ethical requirements and the public’s expectations. Informed electronic consents can ensure personal health data is available at the right time, in the right place, for the right person.

Far from being an obstacle to data flow, informed consent assures “data liquidity” and “data integrity”. Informed consent eliminates the need for expensive, complex, and cumbersome legal agreements among stakeholders involved in HIE. Further it assures consumer trust along with data and claims integrity.

We urge decision makers, lawmakers, and policy makers to work diligently to make sure our national health care systems honor what patients want, what patients need, and what patients expect at every level.
Your Medical Records Aren't Secure

The president says electronic systems will reduce costs and improve quality, but they could undermine good care if people are afraid to confide in their doctors.

By DEBORAH C. PEEL

I learned about the lack of health privacy when I hung out my shingle as a psychiatrist. Patients asked if I could keep their records private if they paid for care themselves. They had lost jobs or reputations because what they said in the doctor's office didn't always stay in the doctor's office. That was 35 years ago, in the age of paper. In today's digital world the problem has only grown worse.

A patient's sensitive information should not be shared without his consent. But this is not the case now, as the country moves toward a system of electronic medical records.

In 2002, under President George W. Bush, the right of a patient to control his most sensitive personal data—from prescriptions to DNA—was eliminated by federal regulators implementing the Health Information Portability and Accountability Act. Those privacy notices you sign in doctors' offices do not actually give you any control over your personal data; they merely describe how the data will be used and disclosed.
In a January 2009 speech, President Barack Obama said that his administration wants every American to have an electronic health record by 2014, and last year's stimulus bill allocated over $36 billion to build electronic record systems. Meanwhile, the Senate health-care bill just approved by the House of Representatives on Sunday requires certain kinds of research and reporting to be done using electronic health records. Electronic records, Mr. Obama said in his 2009 speech, "will cut waste, eliminate red tape and reduce the need to repeat expensive medical tests [and] save lives by reducing the deadly but preventable medical errors that pervade our health-care system."

But electronic medical records won't accomplish any of these goals if patients fear sharing information with doctors because they know it isn't private. When patients realize they can't control who sees their electronic health records, they will be far less likely to tell their doctors about drinking problems, feelings of depression, sexual problems, or exposure to sexually transmitted diseases. In 2005, a California Healthcare Foundation poll found that one in eight Americans avoided seeing a regular doctor, asked a doctor to alter a diagnosis, paid privately for a test, or avoided tests altogether due to privacy concerns.

Today our lab test results are disclosed to insurance companies before we even know the results. Prescriptions are data-mined by pharmacies, pharmaceutical technology vendors, hospitals and are sold to insurers, drug companies, employers and others willing to pay for the information to use in making decisions about you, your job or your treatments, or for research. Self-insured employers can access employees' entire health records, including medications. And in the past five years, according to the nonprofit
Privacy Rights Clearinghouse, more than 45 million electronic health records were either lost, stolen by insiders (hospital or government-agency employees, health IT vendors, etc.), or hacked from outside.

Electronic record systems that don't put patients in control of data or have inadequate security create huge opportunities for the theft, misuse and sale of personal health information. The public is aware of these problems. A 2009 poll conducted for National Public Radio, the Kaiser Family Foundation and the Harvard School of Public Health asked if people were confident their medical records would remain confidential if they were stored electronically and could be shared online. Fifty nine percent responded they were not confident.

The privacy of an electronic health record cannot be restored once the contents are sold or otherwise disclosed. Every person and family is only one expensive diagnosis, one prescription, or one lab test away from generations of discrimination.

The solution is to insist upon technologies that protect a patient's right to consent to share any personal data. A step in this direction is to demand that no federal stimulus dollars be used to develop electronic systems that do not have these technologies.

Some argue that consent and privacy controls are impractical or prohibitively costly. But consent is ubiquitous in health care. Ask any physician if she would operate on a patient without informed consent.

There is no need to choose between the benefits of technology and our rights to health privacy. Technologies already exist that enable each person to choose what information he is willing to share and what must remain private. Consent must be built into electronic systems up front so we can each choose the levels of privacy and sharing we prefer.

My organization, Patient Privacy Rights, is starting a "Do Not Disclose" petition so Americans can inform Congress and the president they want to control who can see and use their medical records. We believe Congress should pass a law to build an online registry where individuals can express their preferences for sharing their health information or keeping it private. Such a registry, plus safety technologies for online records, will mean Americans can trust electronic health systems.

Privacy has been essential to the ethical practice of medicine since the time of Hippocrates in fifth century B.C. The success of health-care reform and electronic record systems requires the same foundation of informed consent patients have always had with paper records systems. But if we squander billions on a health-care system no one trusts, millions will seek treatment outside the system or not at all. The resulting data, filled with errors and omissions, will be worth less than the paper it isn't written on.
Questions Consumers Should Ask about the Hidden Dangers of Online Health and Medical Marketing

Growing numbers of Americans—up to 80 percent according to some estimates—are turning to online sources in search of medical information and advice. From “general practitioners” such as WebMD to “specialists” such as Diabetic Connect, from Facebook pages (ADHD Moms, Breakaway from Cancer) to YouTube (GrowthHormoneTherapy, Parkinson’s Matters), “digital doctors” abound. The emergence of abundant and accessible medical resources online is often hailed as ushering in a new “Health 2.0” era. Consumers are increasingly described as empowered “e-patients,” who can also rely on social media and online communities for advice and support. But while the explosion of medical information services online, including via mobile devices, do provide substantial benefits, this marketplace is being shaped—largely invisibly—by pharmaceutical and healthcare marketers. Drug companies and other medical advertisers will spend nearly $1 billion in 2010 on marketing online—a figure that is expected to reach $1.52 billion by 2014.

In the online health arena, it’s increasingly difficult to determine where the advice ends and the marketing begins. Is that health expert we encounter online really an independent professional, or merely a paid and undisclosed spokesperson for a pharmaceutical company? Is the editorial information written to provide you with an objective discussion of a health problem, or to lure you to ask your doctor for a specific drug brand that advertises on the site? And what about the health information we might share online, either through registering for a particular site, or personal details we might happen to disclose in a social network? Or any of the data collected invisibly about us for so-called online profiling and tracking. Right now, it is impossible to determine precisely how site operators or their third-party affiliates might use that information. How many of us have read those obscure privacy policies on health and pharma sites, which allow for unconstrained use of our health information?

Here are a number of questions that consumers should ask—of themselves, of their online healthcare information providers, and especially of the pharmaceutical marketing industry that sponsors so many of the online health resources:

1. Is Behavioral Targeting Data Collection Conducted on the Site? The privacy threat posed by behavioral targeting, in which marketers deliver marketing based on the stealthily observed and compiled activities of consumers online, has been amply documented. But when the behavior in question extends into the sensitive area of
personal health, with symptoms and searches for treatments and cures added into the profiling and targeting mix, then the advertising practices are invasive. Before even entering a health-related website, then, we should ask, “Are my actions and inquiries being monitored? Will the content I view, and the ads and even information I receive, be shaped by such data-collection practices?” More than merely rhetorical questions, the answers to these queries should determine whether or not a particular health-related site is safe to enter, and health websites should make their data collection and user-profiling practices clear: How much data is collected from site visitors, and how is that information used? Consumers should have the right to have a choice—and be able to “opt-in” before any data can be harvested for targeting.

2. **Does this site offer marketers “Condition Targeting?”** An especially cynical variation on the behavioral targeting theme is the practice of condition targeting. Many health websites offer advertisers the ability to target an individual consumer based on their expressed or implied concern about an illness, including for sensitive concerns as depression, COPD, and diabetes. When those afflicted with an illness are attracted to sites that promise information and treatment, they aren’t told they have become targets for condition-specific digital marketing. And in the face of such manipulative marketing, the obvious question must be asked: What data on an individual user are being collected and how are they used?

3. **Is My “Patient Journey” Being Followed Online by Health Marketers?** Another aspect of medical targeting is the technique of sequential messaging, in which ads are personalized not simply for particular conditions or individuals, but for the specific stages of what health marketers like to call the “patient journey” online. Health consumers are monitored and analyzed as they go online by digital marketers, who can determine the phase of a person’s interest in a problem (such as someone looking for general information who then explores specific treatment options). Tailored for individuals as they move through the stages of diagnosis, treatment, and recovery from a particular illness or condition, this approach to medical marketing raises fundamental privacy issues.

4. **Is this “Unbranded Site” About a Health Concern Really a Drug Company Promotion?** Pharmaceutical companies are bankrolling so-called “unbranded” websites that allegedly offer consumers objective information about a health issue. Sometimes called “disease awareness” websites by medical marketers, their ultimate goal is to encourage consumers to ask their physician to order a specific brand drug or treatment. While the sponsoring drug company may have its name in the equivalent of online “fine-print,” consumers need to be clearly informed they are interacting with a digital infomercial. In other words, ask if this website may be hazardous to your health.

5. **Is the Person Discussing a Health Problem or Treatment Really Independent or a Paid Spokesperson?** “Nine out of ten doctors” may recommend a particular health product, and individual patients may swear to its effectiveness, but the Internet is full of testimonials and advice that are little more than advertisements, in that the spokespersons involved have been compensated for their statements. Existing regulations require
disclosure of paid endorsements, but such arrangements are often buried in a site’s corporate fine print. Is that YouTube testimonial about a health problem or treatment from a “real” person not affiliated with the drug company—or from someone on its payroll? It is incumbent upon consumers, then, to evaluate the product testimonials they encounter online in an effort to distinguish between the unsolicited endorsements and sponsored statements.

6. **What Happens to My Information When I Agree to “Free” Offers and Use Online “Discount” Coupons?** Sometimes the most expensive items on the Internet are free, in that consumers must surrender personal information in order to take advantage of them. The online healthcare arena is replete with “free newsletters,” “discount coupons,” and the like, virtual “loss leaders” that are designed to serve as data-capturing devices. In view of the loss of privacy that such offers entail, consumers must ask themselves, “Can I really afford to accept this offer?”

7. **Have drug companies used forms of physician-targeted digital marketing—e-Detailing—to get my doctor to promote their brands?** The long-established practice of “detailing”—in which pharmaceutical sales reps are deployed to meet with doctors to explain the benefits of particular medications, and to offer free samples and other inducements to increase sales of those products—has now moved online. Armed with information about his or her practice, marketers can engage in new forms of “physician targeting” that serve only to add to the skyrocketing cost of pharmaceuticals. Smart consumers who have already learned to ask their doctors about generic alternatives to costly brand-name drugs now have another question to ask: “Is this prescription based on my health needs, or is it the result of pharmaceutical marketing?” (And on a related note, patients might want to consult ProPublica’s “Dollars for Doctors” database, which lists physicians who have received promotional payments from seven of the largest drug companies.)

8. **What Do Digital Marketers Learn When They Help Provide Electronic Health Records?** The move from cumbersome paper records to online storage and retrieval of medical records and health insurance data has benefits for patients and practitioners alike. But electronic health records (EHR) records, especially in private hands and across wide area networks, raise many privacy concerns. Two of the largest online advertising companies—Google and Microsoft—offer consumers EHR’s (Google Health and Microsoft’s HealthVault), and also pitch their marketing clout to leading pharmaceutical and other medical advertisers. Consumers must ask themselves: are these services adding even more data points to the growing number of interactive health marketing campaigns?

9. **Has the Drug Ad Been Developed using Neuromarketing?** One of the latest developments in advertising, neuromarketing, draws on the techniques of neuroscience to measure consumer response to advertising, with the ultimate goal of crafting commercial messages that directly influence one’s subconscious mind. Leading online advertisers are using the latest techniques to directly influence the behavior of our brains, bypassing the rational decision-making process consumers rely on to make informed decisions. Ads for powerful and expensive drugs pitched to us via new forms of subliminal persuasion
require consumer protection safeguards.

10. Are medical marketers monitoring what I do on Social Media? One of the most disturbing aspects of the Web 2.0 revolution is that it has given rise as well to Surveillance 2.0. Increased user participation in the creation of online content, in other words, has given advertisers and market researchers unprecedented access to consumer interests and tastes. In the process, through data-collection and -analysis technologies that monitor social networks and other forms of user-generated content, marketers have gained access to vast amounts of personal information. Such data are used to formulate advertising that is often delivered—in various forms—over the very same platforms on which consumers have so willingly expressed themselves. Even with the social media movement well under way, it’s still not too late for participants to ask such questions as, “How can I be sure that the personal information that I share with others in online conversations won’t be used for marketing purposes? How do I know that the ‘peers’ with whom I discuss health matters aren’t also being targeted via social media marketing techniques involving ‘peer-to-peer,’ viral and ‘word-of-mouth’ advertising?”

11. Do Privacy Policies on Health Sites Really Protect My Privacy? In general, online privacy statements have been doubly disastrous: virtually no one reads them, and even if they did, the lengthy, complex documents are largely inscrutable. From the opening “We value your privacy” to the closing “These terms and conditions are subject to change,” it’s never clear just what information is protected and what is fair game for outside interests to collect and analyze. Pharmaceutical and health-oriented websites, handling sensitive information as they do, should be held to the highest privacy standards. And users of these sites should be able to find clear, direct answers to the basic privacy questions: What kinds of data are collected? How is this information used? How can I affirmatively decide to avoid these practices altogether before data is collected, and thus keep my information confidential?

12. Have Online Marketing Techniques Been Used to Drive Emotional Responses to Drug Ads? Direct-to-consumer drug advertising on TV has raised concerns about the use of pleasing imagery and skilled actors to promote the sales of prescription drugs. (Remember that colorful butterfly that darts across the screen as a voice-over provides you with the risk and adverse-condition information?) Digital ads are developed using techniques purposefully designed to more effectively tap into a consumer’s interests and concerns, including through interactive applications that “immerse” a consumer. The webpage you may go to can be expressly created just for you as well, in order to make it more effective for marketing. Pharmaceutical and health marketers should disclose what digital ad techniques they use to target consumers.

13. Is the risk information about a drug prominent and in detail on an online pharmaceutical marketing site or application? Many pharma marketers are
trying to replace what’s known as risk and “fair balance” information about a drug’s side effects or shortcomings with just a link and a few words of explanation. They argue that digitally savvy consumers know they can click to learn more about a product. But given all the techniques used online by medical advertisers to encourage a consumer to pay attention to engaging and interactive marketing, ensuring the risk information remains
Competition and antitrust issues on the Internet
Googleopoly VI* Seeing The Big Picture:
How Google is Monopolizing Consumer Internet Media & Threatening a Price Deflationary Spiral & Job Losses in a $Trillion Sector

Why the Facts and the Economic/Societal Stakes Warrant:
The U.S. DOJ Filing a Sherman Section 2 Antitrust Case & The European Union Filing a Section 102 Statement of Objections

By Scott Cleland**
President Precursor LLC
scleland@precursor.com

September 13, 2010

* See Appendix B for links to Googleopoly I-V research series.
** The views expressed in this presentation are solely the author’s and not the views of any Precursor LLC clients. See Scott Cleland’s full biography at: http://www.precursor.com/bio_long.htm
Outline

I. Executive Summary
II. How Lax Antitrust Enforcement Facilitated Googleopoly
III. How Google Increasingly is the Internet
IV. How Google Violates Antitrust Law
V. Googleopoly’s Deflationary Impact on Economic Recovery
VI. Conclusions & Recommendation

Appendix: Bio & Googleopoly Research
I. EXECUTIVE SUMMARY
Executive Summary:  
Recommendation & High-Level Conclusions

Recommendation:
• The facts and stakes warrant the U.S. DOJ filing a Sherman Section 2 Antitrust Case and the EU Filing a Section 102 Statement of Objections – against Google Inc. for monopolizing consumer Internet media services.
  – Since Google increasingly is the Internet for info access and distribution, and also is increasingly monopolizing the consumer Internet media ecosystem with a systematic monopolization strategy, a broad antitrust case is warranted, because event-specific investigations/actions are a losing antitrust game of ‘whack-a-mole.’

High-Level Conclusions:
• Lax antitrust enforcement tipped Google to monopoly & facilitates monopolization of consumer Internet media.
• Google’s monopoly platform increasingly is supplanting and dominating the consumer Internet media ecosystem.
• There is more at stake than competition from a global information access bottleneck; Googleopoly threatens economic growth, jobs, privacy, intel. property, a free press, fair elections, cyber-security, & sovereignty.
• Only Google has a billion user audience, ~all information/advertisers/publishers, & a free-info business model that can sustain pervasive predatory free info/products/services long term. There’s no net-economic-growth or net-job-creation in a “free” Internet sector model -- only: a deflationary price spiral; net negative growth, property devaluation, job losses, and monopolization. Over 20 industries, 200+ US/EU companies, and hundreds of thousands of jobs are at risk from Googleopoly’s anti-competitive price deflationary spiral.
• The consumer does not win long-term from monopoly-control over “free” information access & distribution.
Executive Summary: Additional Conclusions

1. Google is a vastly more serious antitrust threat to consumers and the economy than Microsoft, because the DOJ blocked Microsoft from extending its monopoly vertically into the broader economy, while antitrust authorities have unwittingly aided and abetted Google’s vertical monopolization of vast parts of the broader economy.

2. Lax antitrust enforcement allowed dominant Google search to acquire: YouTube’s dominant video-streaming, DoubleClick’s dominant display ad-serving/analytics, and AdMob’s dominant mobile advertising -- to create a dominant Google TV global “monocaster” platform for all types of IP devices with 80% of the video streaming audience and dominance of IP video views/minutes viewed. Only Google TV has no media concentration limits.

3. The Internet’s greatest strength is also its greatest weakness, in that the Internet’s universality naturally leads to extreme centralization, concentration and market power. Thus Google increasingly is the Internet for most.

4. Google has systematically assembled all the building blocks in the “stack” of necessary capabilities to become the dominant platform of the consumer Internet media ecosystem: a winner-take-all dynamic; omniscient mission and omni-directional ambition; omnivorous info collection; Internet omnipresence; Internet-scalable infrastructure; omnifarious products, services & info types; Internet behavior omniscience; and omnivorous ecosystem share.

5. Google has unique “Total Information Awareness Power” where it collects, records, stores, and analyzes most all Internet activity: all the world’s information and all market information of usage, traffic, supply and demand; and permission-less profiles of users’: personal identifications, locations, intentions, and associations.

6. Google’s monopoly power is lasting because of re-enforcing spheres of monopoly influence -- a monopoly platform surrounded by: 75+ acquisitions; many satellite companies financially dependent on Google for search monetization; thousands of publisher revenue-share “partners;” and a phalanx of free info, products and services.

7. Google’s secret weapon is its “deep tracking inspection” of everything that passes through Google’s cloud, where “innovation without permission” means that Google has to ask no one for permission to use the derivative tracking metadata from anyone: publisher partners, advertiser clients, competitors, proprietary owners or users.

8. Google is not an honest broker in search; it hides multiple serious conflicts-of-interest.
II. HOW LAX ANTITRUST ENFORCEMENT FACILITATED GOOGLEOPOLY
Why Google’s a Greater Monopolization Threat Than Microsoft Was Generally Lax Antitrust Enforcement

DOJ Prevented Vertical Extension of Microsoft’s Monopoly by Blocking Intuit and Prosecuting on Netscape

DOJ*/FTC Tipped Google to Monopoly & Facilitated Vertical Monopolization in Approving YouTube, DoubleClick & AdMob

Microsoft

100%

Vertically or Other-industry Share

Fully Competitive Vertical Marketplace
Maintained with Antitrust Enforcement

1998 DOJ Filed Sherman Act Monopolization Case over Netscape Browser

1995 DOJ blocked Microsoft–Intuit Expansion into financial services

Horizontal Monopoly

Horizontal or In-industry Share 0%

100%

Google

100%

Vertically or Other-industry Share

At Risk Competitive Vertical Marketplace
DOJ*/FTC Tipped Google to Monopoly by Not Blocking Monopolizing Acquisitions

Video
Analytics
Mobile

Horizontal Monopoly & Vertical Monopolization

Horizontal or In-industry Share

0%

100%

9/13/2010

Scott Cleland -- Precursor LLC
How Google’s Acquisitions Have Substantially Lessened Competition

Google’s race to lock up market power before the lax antitrust enforcement window closes

Key Google Acquisitions in Italics; Googleopoly in Red; Competitive Consumer Internet in Green

Competitive Consumer Internet Marketplace

- News/Blogging Vertical: Feedburner, Blogger
- Financial Vertical: Global IP Solutions, Simplify Media
- Sports & Entertainment Vertical: ITA Software
- Travel Vertical: Adscape, Zynga, Investment, Jaiku, Jambol
- Shopping Vertical: Dodgeball, Picassa, Zingku, Picnik, Aardvark, Slide, Jambol Like.com, Angstro, Social Deck
- Games: Green Border, Peakstream
- Social Media: CAPTCHA, Apjlet, Postini, DocVerse, Agnilux, Bump Technologies, Instantiators
- Cloud Computing: Grand Central, Postini, Gizmo5
- Integrated Communications: Where2, Keyhole, Endoxon, Image America
- Mapping/Location Info: Urchin, YouTube, Trendalyzer, DoubleClick, AdMob
- Traffic Analytics: Zipdash, Measure Map, YouTube, Trendalyzer, DoubleClick, AdMob
- Web Behavior Tracking: dMarc Broadcasting, Omnisio, YouTube, On2, Episodic
- Video Streaming Audience: DoubleClick, AdMob
- Display Ad-serving: DoubleClick, AdMob
- Display Publishing Tools: Mobile Search
- Mobile Search: Android, AdMob
- Search Advertising: Applied Semantics, AdMob, Invite Media, Jaiku, Teracent
- Search: In 2010 alone: Aardvark, reMail, PlinkArt, Metaweb, Like.com
- Information Metadata: Google Book Digitization, YouTube, Metaweb
- World’s Information: Keyhole, Image America, Book Digitization, YouTube, Metaweb
- Web Publishers: YouTube, DoubleClick
- Internet Advertisers: dMarc Broadcasting, YouTube, DoubleClick, AdMob
- Internet Users: YouTube, DoubleClick, AdMob

Estimated Consumer Internet Market Share

0% 100%
Why Competition Isn’t “One Click Away” Because of the “Internet Choice Paradox”

Advertisers not Consumers Pay for Internet Content
Consumers are the Product Advertisers & Publishers Essentially ‘Buy’ from Google
So Competition is Not “One Click Away” for Real Customers: Advertisers/Publishers

Consumer Info Choice is “one click away”

Internet

Cloud of Content

GLOBAL
Scale & Scope
Efficiencies

Minimal Transactional Friction Costs

Advertiser/Publisher Customers Face Googleopoly & Have Little Choice
To Reach Most Users Thus
“Competition is NOT a Click Away” for the Real Paying Customers

“Advertising is the lifeblood of the digital economy.” Google Blog 3-11-09

Googleopoly Bottleneck*

Google largely controls access to consumers

* Barriers to entry – costly/difficult to aggregate global segmented networks of:
  • Viewers
  • Advertisers
  • Websites
“Network effects” reinforce dominance

Free
Access to reach any content of choice

Costly
Access to reach the desired users

9/13/2010 Scott Cleland -- Precursor LLC
How Googleopoly’s Core Virtuous Circle & Perpetual Feedback Loop Works

The Most Important Network Effect Antitrust Enforcers Have Under-appreciated

“So more users more information, more information more users, more advertisers more users, more users more advertisers, it’s a beautiful thing, lather, rinse repeat, that’s what I do for a living. So that’s [what] someone alluded to – ‘the engine that can’t be stopped.’” Jonathan Rosenberg, Google Sr. VP 2-27-08
How YouTube Acquisition Helped Tip Google to Monopoly

~75% of Google’s Search Market Share Gains 7-06 -- 7-10 Were YouTube

YouTube is now second largest generator of searches in the world & 25% of all Google searches

*Google Acquired YouTube 11-06

*(DOJ asked for no second request for information)*
How DoubleClick Acquisition Tipped Google to Monopoly
Acquired Most All the Users, Advertisers & Publishers Google Didn’t Have
4-1 FTC Approval Created Googleopoly Virtuous Circle & Perpetual Feedback Loop

2. Merger Combines # 1 & # 2 Internet Audiences (Demand)

3. Merger Combines # 1 & # 2 Online Ad Client Bases (Supply)

~650m Google Users

Google thousands of advertiser clients

DoubleClick Top ~1500 advertiser clients

~800m DoubleClick Ad Viewers

DoubleClick 17 of top 20 Websites +

Google million + AdSense network of websites

= New Market Power from Merger

Content Providers

Users

Advertisers

4. “Cornered:”

Search
Ad-Serving
Behavior Metadata
Performance Analytics
Ad Brokering/Ad Exchange

1. Merger Combines # 1 & # 2 Internet Content Networks (Currency)
How FTC Approval of AdMob Ceded Google a Mobile Ad Monopoly
Created a New Bottleneck For Advertisers/Publishers Entering In-App Mobile Advertising

PC-Advertiser/Publisher Entry into Mobile In-App Advertising

Potential Competition
Yahoo (with 300k advertisers) & Microsoft (100k) are not material competitors in In-App Mobile Ad Market

Actual Competition
No actual competitor is estimated to have >~20,000 advertisers

Google
Google DoubleClick-YouTube has ~1,500,000 advertisers, (UBS/NYT), ~100 times more advertisers than any other actual in-app mobile provider. Google unilaterally, without customer permission, changed the ad defaults for all their advertising customers to opt-in for Google’s mobile ad serving – thus leveraging its dominant search advertiser base and ad inventory in PC advertising into the in-app mobile advertising market. (Appitalism)

No Bottleneck: Google & AdMob Competing
Google Competitors Have 75% Share of In-App Ads
AdMob has First-Mover Advantage & Best Offering

No Merger
Market Share: 25% 50% 25%

With Merger

Bottleneck with Google-AdMob
Google Merges to 75% Monopoly Share of In-App Ads
Eliminates Largest & Only Major In-App Ad Competitor

Google already has >95% share of the mobile search market per Netmarketshare.com

Sources: Precursor LLC estimates; Googleopoly V; UBS; NYT; Appitalism; AdGooRoo.

Scott Cleland -- Precursor LLC

9/13/2010
What’s One Result of Lax Antitrust Enforcement of Google?

Google TV: Global Internet Monocaster

Controlling access to most Internet users, publishers, & advertisers, is it surprising: Google-YouTube owns ~80% of video streaming audience? Google dominates online video sessions viewed & viewed minutes?

ComScore Video Metrix Chart – July 2010

<table>
<thead>
<tr>
<th>Property</th>
<th>Total Unique Viewers (000)</th>
<th>% of Unique Viewers</th>
<th>Viewing Sessions (000)</th>
<th>% of Viewing Sessions</th>
<th>Minutes per Viewer</th>
<th>% of Viewed Minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Internet Audience</td>
<td>178,148</td>
<td></td>
<td>5,234,655</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Google Sites</td>
<td>143,226</td>
<td>80.4%</td>
<td>1,884,498</td>
<td>36.0%</td>
<td>282.7</td>
<td>32.1%</td>
</tr>
<tr>
<td>2 Yahoo Sites</td>
<td>55,107</td>
<td>30.9%</td>
<td>238,322</td>
<td>4.6%</td>
<td>28.6</td>
<td>3.2%</td>
</tr>
<tr>
<td>3 Facebook .com</td>
<td>46,571</td>
<td>26.1%</td>
<td>166,186</td>
<td>3.2%</td>
<td>18.3</td>
<td>2.1%</td>
</tr>
<tr>
<td>4 Microsoft Sites</td>
<td>45,558</td>
<td>25.6%</td>
<td>219,149</td>
<td>4.2%</td>
<td>40.2</td>
<td>4.6%</td>
</tr>
<tr>
<td>5 VEVO</td>
<td>43,911</td>
<td>24.6%</td>
<td>202,091</td>
<td>3.9%</td>
<td>68.5</td>
<td>7.8%</td>
</tr>
<tr>
<td>6 Fox Interactive Media</td>
<td>38,136</td>
<td>21.4%</td>
<td>164,760</td>
<td>3.1%</td>
<td>27.2</td>
<td>3.1%</td>
</tr>
<tr>
<td>7 Turner Network</td>
<td>33,442</td>
<td>18.8%</td>
<td>107,793</td>
<td>2.1%</td>
<td>25.3</td>
<td>2.9%</td>
</tr>
<tr>
<td>8 Viacom Digital</td>
<td>30,715</td>
<td>17.2%</td>
<td>70,617</td>
<td>1.3%</td>
<td>44.8</td>
<td>5.1%</td>
</tr>
<tr>
<td>9 Disney Online</td>
<td>28,475</td>
<td>16.0%</td>
<td>64,104</td>
<td>1.2%</td>
<td>6</td>
<td>0.7%</td>
</tr>
<tr>
<td>10 Hulu</td>
<td>28,455</td>
<td>16.0%</td>
<td>153,845</td>
<td>2.9%</td>
<td>158</td>
<td>17.9%</td>
</tr>
</tbody>
</table>
How Did Lax Antitrust Enforcement Create a Monocaster?
Add search dominance with acquisitions dominant in video, display, & mobile!

“How YouTube is a big component of our display revenue, and display is our next big business.” Google CEO Schmidt NYT 9-3-10
“Ultimately our goal at Google is to have the strongest advertising network and all the world’s information.” Google CEO Schmidt 8-23-06

<table>
<thead>
<tr>
<th>World Monocaster Media Concentration Equation</th>
<th>Google’s Extreme Global Vertical Media Concentration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>Dominant ~Remote Control, ~TV Guide, User Audience: 620m daily</td>
</tr>
<tr>
<td>Search Advertising Dominance</td>
<td>, Advertiser Network, Web Publisher Network</td>
</tr>
<tr>
<td>YouTube</td>
<td>Dominant Online Video Audience, Software, Operating System, Internet Video-casting Infrastructure</td>
</tr>
<tr>
<td>Video Streaming Dominance</td>
<td>Dominant Ad-Serving Software, Display Analytics, &amp; Neilsen-like Tracking &amp; Viewing Measurement</td>
</tr>
<tr>
<td>DoubleClick</td>
<td>Dominant Mobile in-app Ad-Serving Software Combined with Free Android Fastest Growing Mobile Operating System</td>
</tr>
<tr>
<td>Display ad-Serving/Analytics Dominance</td>
<td>80% of video-streaming audience</td>
</tr>
<tr>
<td>AdMob</td>
<td>2 billion monetized views daily</td>
</tr>
<tr>
<td>Mobile Advertising Dominance</td>
<td>160m daily mobile streamed views</td>
</tr>
<tr>
<td>Google TV Network Dominance</td>
<td>45 billion ads served daily</td>
</tr>
<tr>
<td>To All Types of IP Devices</td>
<td>94 of top 100 Ad Age Advertisers</td>
</tr>
</tbody>
</table>
III. HOW GOOGLE INCREASINGLY IS THE INTERNET
How The Internet’s Greatest Strength Is Its Greatest Weakness

How Internet Universality Leads to Centralization, Concentration & Market Power

And Why Google Increasingly is the Internet for More & More People

“What Google has done is simply take every feature in every product on the market and put them all into one system, and then make it available for free.” Brandt Dainow, iMedia Connection 7-31-07

First Mover Advantage: innovation/acquisition

Strong market relative valuation advantage for sector leader

IP is the fastest & most universal global standard ever adopted

Uniquely minimal global border friction or inefficiency

Switching costs & user stickiness from integration, mash-ups, bundling, cookies, passwords, etc.

Centralization

Concentration

Winner Takes All

Market Power Dynamic

Moore’s Law: processing costs halve every 18 months

Metcalf’s Law: value of network is the square of its nodes

Gilder’s Law: bandwidth triples every year

Economies of scale means falling average fixed costs

Network effects: strong get stronger feedback loops

Monopoly & monopsony market power

Scope integration efficiencies mean near zero marginal cost of adding features & free products, services

Leading Examples of this Internet “Winner Take All” Dynamic:

Google: search; Youtube: online video; DoubleClick: Ad-serving & Analytics; eBay: auctions;

Amazon: e-retailing; Facebook: social media; Skype: VoIP; Twitter: real-time-infocast

9/13/2010

Scott Cleland -- Precursor LLC
**Why Google is the Internet Media Ecosystem’s Consumer Platform**

*“Anything that benefits the Internet ecosystem will benefit Google.”* Google’s Peter Greenberger 3-2-10

*“The Internet makes information available; Google makes it accessible.”* Google’s Hal Varian 11-3-09

<table>
<thead>
<tr>
<th>Consumer Internet Ecosystem</th>
<th>Why Google is Emerging as the Consumer Internet Media Ecosystem’s Monopoly Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Omnipotence</strong></td>
<td>The consumer Internet media ecosystem increasingly will determine: what information most people read, view, hear, learn and find; which products and services most people demand, buy or consume; which companies and organizations succeed or fail; and how competitive and diverse the world Internet Media business and environment will be for consumer and voters.</td>
</tr>
<tr>
<td><strong>Omnivorous Ecosystem Share</strong></td>
<td>Google currently commands: ~80% of global searches, 90+% of search advertising revenues, 98% of mobile searches; ~80%+ of unique online video viewers; ~90% share of web and website use analytics; a dominant share of mapping/location usage; only searchable database of most all videos online; only searchable database of millions (12) of digitized books; etc.</td>
</tr>
<tr>
<td><strong>Internet Behavior Omniscience</strong></td>
<td>Google is unique in having “Total Information Awareness” Power as the only entity on earth that can: track most all Internet usage, clicks, views, etc. via tracking of their unique access to 80% of global users and 90% of commercial advertisers and publishers; profiles user identifications, location, intent and associations; and monitor most all market behavior informatio and world’s info.</td>
</tr>
<tr>
<td><strong>Omnifarious Information Types</strong></td>
<td>Most all info types: News, articles, videos, images, maps, pictures, books, shows, movies, songs, blogs, research, presentations, podcasts, emails, documents, desktop hard-drives, voice-prints, face-prints, click-prints, personal info, health records, Financials, contact lists, group lists, addresses: emails, domains, WiFi SSID, Mac; phone numbers, Analytics, graphs, charts, languages, histories, dictionaries, trends, prices, etc.</td>
</tr>
<tr>
<td><strong>Internet-Scalable Infrastructure</strong></td>
<td>Only Google has only Internet infrastructure (datacenters, databases, storage, servers &amp; bandwidth) designed to fully scale with Internet growth; Google’s BigTable distributed database design can store, process and design virtually unlimited info; Google’s server-virtualization design is world’s most efficient; Google’s fiber network carries more IP traffic than any in the world.</td>
</tr>
<tr>
<td><strong>Internet Omnipresence</strong></td>
<td>Only Google serves most all Internet users (~80%), advertisers (~90%) &amp; publishers (~90%); Only Google translates 57 languages, comprising ~90% of Internet users</td>
</tr>
<tr>
<td><strong>Omnivorous Information Collection</strong></td>
<td>Google’s self-described “omnivorous” search engine is uniquely universal in being designed to incorporate all types of info and also a searcher’s “total context” i.e. location, experience, intent</td>
</tr>
<tr>
<td><strong>Omni-directional Ambition Omniscient Mission</strong></td>
<td>Unique mission: “organize the world’s information and make universally accessible and useful,” routinely organizing others’ information that’s copyrighted, proprietary, private, secret, sensitive</td>
</tr>
<tr>
<td><strong>“Winner Takes All” Internet Dynamic</strong></td>
<td>Internet universality naturally facilitates Google’s centralization, concentration, &amp; market power</td>
</tr>
</tbody>
</table>
How Google’s Mono-mediary Hub Platform is an Internet Media Bottleneck Or When Googleopoly Meets Googleopsony

**Supply of Consumer Internet Media**

Google dominates how much revenue info can generate

Google’s dominance forces wholesale info prices towards free

**Distribution Competition for Internet Media?**

~90% of Advertisers

Advertisers objected to Google-Yahoo, auction opacity

26 Network Effects (Googleopoly II)

DOJ: Google is Dominant in: Search Advertising, Search Advertising Syndication
(DOJ Statement blocking Google-Yahoo ad deal)

Googleopoly

“Black Box” Auction

Googleopsony*

Control derivative uses of digital info

Mono-mediary

Less Quality Integrity & Diversity

**Demand from Internet Consumers**

Consumers Increasingly Will Discover Only What Google Prioritizes

70+% of Search Ad Audience

90+% Display Ad Global Reach

70+% of U.S. Searchers

80-90% of Global Searchers

Largest Information index much is proprietary, maps, video, etc.

DOJ: “The seller of an incomplete database... cannot compete with the seller of a comprehensive product”

(DOJ letter to Court on Book Settlement)
How Google Uniquely Has “Total Information Awareness” Power

“We are very early in the total information we have within Google… we will get better at personalization.” Google CEO, FT 5-22-07

*Information now available for: Googleopoly's leverage, law enforcement subpoena, national security access, & hackers to steal

---

**Personal Identifications**
IP addresses via Search/Analytics/Cookies/Chrome
Email addresses via Gmail scanning & Postini filters
WiFi, SSID & MAC addresses via WiFi wardriving
Phone/mobile #s via search, Android, Voice, Talk
Voiceprint recognition via Goog411/Google/Translate
Face-print recognition via Picassa, Images, YouTube
57 Languages identified via Translate/Google/Video
Home addresses: Maps/Earth/StreetView/Android
Personal info via product/service registrations
Social Security/passport/license #s: Desktop Search
Credit card & bank info: Checkout/Finance/Desktop
Investment in 23andMe enables DNA identification
Health identifiers by Health, Search, Gmail, Books
Click-print IDs via analysis of multiple web histories

**Personal Location**
Android GPS tracks location when no apps running
Search/Toolbar/Android use reveals user’s location
Talk/Voice/Maps/Calendar signal destination plans
Google Goggles recognizes location via Streetview
Search/Earth/Maps/StreetView show favorite places

**Market Information**
Only omnipresent Internet click tracking/analysis
Uniquely see all online advertiser demand/trends
Uniquely comprehensive view of user demand
Unique complete view of publisher ad inventory
Unique view of global supply/demand for prices
Lone access to non-public Google Trends info
First to see new trends/fads/growth inflections
Unique access to unregulated inside information
Universe knowledge of online ad market pricing

**World’s Information**
Trillion web-pages crawled/copied regularly
25,000 sources copied by Google News
12 million books copied by Google Books
90+% movies/TV shows copied by Youtube
~99% satellite images copied by Google Earth
90+% homes in 33 countries videoed StreetView
175 million users gmails copied regularly
57 languages’ content auto-translated via Translate

---

Privacy Invasion Problem

Permission-less Profiling Power

Google’s Total Information Awareness Power

Information Market Power

Antitrust/Monopoly Problem

---

*Personal Intentions*
~75% share of U.S. search; ~90% of European search
Behavioral advertising profile for targeted ad-serving
Intensive interests via iGoogle, Search, Alerts, Reader
Click tracking: Analytics, DoubleClick, YouTube, Chrome
Location interest via Maps, Earth, StreetView, Search
Financial interests: Search/Finance/Portfolios/Shopping
Private drafts via Gmail, Docs, Groups, Desktop Search
Plans via Google Calendar, Gmail, Buzz, Voice, Talk, Docs
Likely votes by party/issue: Search/News/Books/Reader
Health concerns via Health/Search/Books/YouTube/Knoi
Upcoming purchases: My Shopping List/Search/Buzz
Groups knows one’s politics/religion/issue views

*Personal Associations*
Contact lists: Gmail, Buzz, Voice, Orkut, Groups
Interests: iGoogle/Alerts/News/Reader/Groups
Reading: News/Books/Knoi/Reader/My Library
Viewing: YouTube, Video, DoubleClick, Analytics
Friends: Orkut/Picassa/Buzz/Gmail/Talk/Voice
Gathering places: Earth, Maps, StreetView, Android

---

9/13/2010
Scott Cleland -- Precursor LLC

---

20
How Google’s Chief Economist Explains the Market Power Behind Google’s Dominance of Consumer Internet Media

Steve Levy of Wired shares Google Chief Economist Hal Varian’s take on “Googlenomics”*: 

- “Googlenomics actually comes in two flavors: macro and micro. The macroeconomic side involves some of the company's seemingly altruistic behavior, which often baffles observers. Why does Google give away products like its browser, its apps, and the Android operating system for mobile phones? Anything that increases Internet use ultimately enriches Google, Varian says. And since using the Web without using Google is like dining at In-N-Out without ordering a hamburger, more eyeballs on the Web lead inexorably to more ad sales for Google.” [Bolds added for emphasis.]

- “The microeconomics of Google is more complicated. Selling ads doesn't generate only profits; it also generates torrents of data about users’ tastes and habits, data that Google then sifts and processes in order to predict future consumer behavior, find ways to improve its products, and sell more ads. This is the heart and soul of Googlenomics. It's a system of constant self-analysis: a data-fueled feedback loop that defines not only Google’s future but the future of anyone who does business online.” [Bolds added for emphasis.]

- “…Varian believes that a new era is dawning for what you might call the datarati— and it's all about harnessing supply and demand, ”What’s ubiquitous and cheap?” Varian asks. ”Data." And what is scarce? The analytic ability to utilize that data." [Bolds added for emphasis.]

- “Varian, of course, knows that his employer's success is not the result of inspired craziness but of an early recognition that the Internet rewards fanatical focus on scale, speed, data analysis, and customer satisfaction.” [Bold added for emphasis.]

*Steven Levy, “The secret of Googlenomics, data-fueled recipe brews profitability,” Wired Magazine, 5-22-09,
  http://www.wired.com/culture/culturereviews/magazine/17-06/nep_googlenomics?currentPage=all
IV. HOW GOOGLE VIOLATES ANTITRUST LAW
Google’s Monopolization Strategy
“It’s obvious what our strategy should be. It’s to work on problems on a scale no one else can.” Sergey Brin, Wired UK 6-30-09

- **Misrepresent conflicts of interest to build trust as an honest broker.**
  - Google built an ill-gotten critical mass of user trust through systematic misrepresentation of Google’s real interests and by not publicly disclosing serious conflicts of interest that would be considered fraudulent and deceptive if done in the off-line marketplace.

- **Systematically foreclose competition.**
  - Google uses unique market-wide metadata information power to find and buy the most strategic first movers cheap before: a business model can form effectively; *revenue* hits the “hockey stick” growth inflection point; a market can be defined for antitrust enforcement purposes; and others learn what Google knew from analyzing everyone else’s proprietary metadata without permission.
  - Google co-opts and subordinates actual and potential competitors by providing outsourced search, tracking/analytics, and advertising monetization through opaque and supra-competitive revenue-sharing arrangements that create business dependency on Google.
  - Google forces the wholesale price for information access towards zero by copying all information without permission/compensation to make it accessible for free, then forcing an ad-monetization model so that info itself is not valuable, but only access & functionality.

- **Structure opaque derivative markets so Google can be player, referee, scorekeeper & paymaster all at once.**
  - Google’s “auctions” are not auctions between buyers and sellers where the highest price prevails; Google’s auctions are a derivative algorithm that discriminates against bidders to award the ad, not to who bids the most, but to who Google *estimates* has the best probability of generating the most derivative ad clicks and hence revenue for Google. Google also unilaterally sets minimum bid prices.

- **Exclude competitors from information critical to competition.**
  - Google owns and controls uniquely vast and critical datasets (YouTube, Books, Earth/Maps/StreetView, etc.) and makes them publicly accessible and useful to users, but excludes competitive crawling or indexing so competitors cannot offer competitive search results.
  - Google harvests & controls the derivative “metadata” (data on the data) that the dominant Google Internet media platform produces, i.e. the how, what, where, when, how, why & how much of most all the Internet traffic, clicks and behavior that Google uniquely records to allow Google to create unique derivative metadata profiles of individual users, groups, demographic slices, and the market overall.

- **Discriminate predatorily against competitors and “self-deal” in favor of Google info, products and services.**
  - Google detects and impedes emerging search competitors from becoming more competitive by predatory monopoly discrimination using “human raters” to lower their search ranking and increase their price per click so they have to pay more for less & can’t compete;
  - Google self-deals by using Google’s unique knowledge of partners, competitors, and users proprietary/private information to identify, own and then rank critical building block content first, above partners and competitors, so that competitors cannot succeed.

- **Front-run partners and competitors by using their own confidential/proprietary information against them.**
  - Google tracks, records and analyzes most all behavior on the Internet, Google’s “Total Information Awareness Power,” so Google can effectively reverse-engineer the most valuable trade secrets and confidential information from partners and competitors, i.e. their confidential client lists (users, advertisers), *their actual measured* strengths and weaknesses, plans, strategies, and tactics.
How Google Rigs their Info-Casino Game – So they Can’t Lose

• Google deals itself Aces that are hidden in its sleeve.
  – Google manually ranks Google-owned content first: Maps, YouTube, Mobile, etc., despite representations that Google “never manipulates search rankings to put our partners higher in search results”
• Google deals its competitors bad cards opaquely from bottom of the deck.
  – Google’s “human raters” opaquely and mysteriously assign “quality scores” so certain competitors rank low in results and have to pay more to get less traffic
• Google alone sees & counts everyone’s else’s cards -- so they can’t lose.
  – Only Google tracks all players information, connections, interests, click-paths
  – Only Google profiles/categorizes each user into demographic target groups
  – Only Google can reverse-engineer publishers’ audience and advertiser lists to create Google content/products/services that front-run/skim off publishers
  – Only Google knows all advertiser demographic demand so Google can front-run its publisher-partners with Google-owned content/products/services
• Google alone decides: who can play which hands; what the specific ante is.
  – Google alone: decides who can bid on which keywords, & sets price minimums
• Google runs a ‘black box’ – no transparency to keep the dealer honest.
  – Google excludes competitors from the game who could spot double-dealing
  – Google alone keeps score and counts clicks with no one watching
  – Google alone decides the worth of each click type with no one watching
Why Google is Not an Honest Broker
It Hides Multiple Serious Conflicts-of-Interest

- Google may have devised the most conflicted business model ever – in funneling and ranking all the world’s information, for most all the world’s users, advertisers, and publishers, through one single gateway, for money, without anyone’s permission, and without any independent third-party accountability mechanisms.
- Who does Google work for?
  - Google users whom Google claims it works for, but who don’t pay Google for most anything?
  - Google advertisers who actually are Google’s real customers or users who Google claims it works for?
  - Google publishers, who Google calls its “partners,” since they revenue-share with Google?
  - Google shareholders whose votes don’t matter since Founders granted their stock 10 votes per share?
- Which Google role rules and how are Google’s conflicting roles represented and/or resolved?
  - Google as player/competitor in owning content, products and services?
  - Google as referee in manually setting website quality scores or censoring info from search/advertising?
  - Google as scorekeeper in ranking everyone’s information?
  - Google as paymaster in running “derivative non-auctions” for most all of the industry?
  - Google as proprietary owner of the dominant consumer Internet media platform?
- Unlike every other public broker role in finance, real estate, auctions etc. -- which must disclose and publicly manage conflicts-of-interest fairly in order to operate as an “honest broker” and avoid charges of misrepresentation or fraud -- Google does not even publicly acknowledge the existence of its multiple serious conflict-of-interest, or that they could potentially harm consumers, customers, or the public.
# How Google is Systemically Anti-Competitive

## Consumer Internet Ecosystem Building Block Capability “Stack”

| Consumer Internet Ecosystem Omnipotence | Only Google has self-described “king maker” power to determine what information or applications are found, used, read, viewed, etc., & which businesses succeed or fail on the Net. |
| Omnivorous Ecosystem Share | Google has leveraged acquired dominance of users, advertisers, publishers, and exclusionary information practices to dominate search, search advertising, Mobile advertising, video streaming; display ad-serving/tools/analytics, Mapping, video streaming, and web behavior tracking. |
| Internet Behavior Omniscience | Google’s “innovation without permission” is viewed by Google as cart blanche to collect whatever information it can on its users, partners, competitors without respect to privacy, IP or confidentiality. |
| Omnifarious Information Types | Google includes as many information types as it can in its universal search so it can either have unique or exclusive information so users must use Google as their search engine. |
| Omnifarious Products & Services | Google predatorily subsidizes new products & services in order to commoditize search complements to foreclose actual and potential competition to Google. |
| Internet-Scalable Infrastructure | No other company has the monopolistic vision of designing an infrastructure to scale with the entire internet nor will any other company be willing to take the security, business, property, and privacy risks of Google’s “BigTable” -- all-eggs-in-one-basket design. |
| Internet Omnipresence | Monopoly-tipping acquisitions: YouTube, DoubleClick, & AdMob, network effects, information exclusions, and monopoly discrimination, self-dealing and front-running ensure that no competitor can aggregate a comparable share of Internet users, advertisers and publishers – the vortex of Google’s monopoly power. |
| Omnivorous Information Collection | DOJ on Google Book Settlement: “The seller of an incomplete database... cannot compete effectively with the seller of a comprehensive product.” Google actively prevents competitors from crawling some of the largest stores of the World’s information – YouTube’s videos, Google’s Maps & 12 million digitized books – publicly accessible to users. |
| Omni-directional Ambition Omniscent Mission | Free market competition depends on rule of law, and contract and anti-fraud enforcement; No law abiding company can compete against a scofflaw which abuses IP, contracts, confidentiality, & privacy for competitive advantage. |
| “Winner Takes All” Internet Dynamic | To the winner go the spoils: Google takes-out first-mover nascent competitors before market definition & revenue competition can form; Self-deals Google content top search result; “Human raters” punish competitors with low quality scores, low rankings, higher prices per click; Front-run publishers with new content/products/services based on publishers’ proprietary information. |
How Google Has Re-enforcing Spheres of Monopoly Influence

**Most of Internet is Either on Google’s Payroll or Undercut by its Free Info/Products/Services**

“I think the solution is tighter integration. In other words, we can do this without making an acquisition. The term I’ve been using is ‘merge without merging.’ The Web allows you to do that, where you can get the Web systems of both organizations fairly well integrated, and you don’t have to do it on exclusive basis.” Google CEO Schmidt 1-7-09

**Black Box Monopoly Platform:**
- Search Engine; Auctions; Quality Score
- “Human Raters;” Exclusive info/ Metadata

**Acquisitions:**
- YouTube = ~80% Video streaming audience share, quarter of all search; DoubleClick = most all users, advertisers, publishers Google did not have, and Dominance in ad-serving and analytics;
- AdMob = ~75% in-app mobile ad share

**Satellite** companies dependent on Google for search monetization:
- AOL, MySpace, Ask.com, Craigslist, and thousands of popular websites

**Partners:**
- Tens of thousands of AdWords and AdSense advertisers and publishers share revenues derived from Google’s opaque pay-per-click “auction” model

**Free Google Content, Products & Services:**
- Search, Images, Videos, Maps, News, Shopping, Gmail, Books, Finance, Translate, Scholars, Blogs, YouTube, Calendar, Photos, Documents, Reader, Sites, Groups, Alerts, Chrome, Desktop, earth, Goog-411, StreetView, Health, Knol, Orkut, Picassa, talk, Voice, iGoogle, etc.

**The Shrinking Competition:** Those companies not:
- Hoping to be acquired by Google;
- Dependent on Google for search monetization;
- “Partners” in Google’s search or display advertising; or Users of Google’s free content, products, & services
How Google Search Discriminates Against Competitors’ Content/Distribution

Google’s Rapidly Extending its Monopoly Via Search-Favored & Free: Google Information, Products & Services

Can’t compete with a search monopoly that ranks/advertises its own info, products & services above everyone else’s

“Search is critical. If you are not found, the rest cannot follow.” Santiago de la Mora, Google Executive, 8-23-09

Digital Information competition to Google

World’s Info made accessible & useful by Google

Google-owned content verticals

Google-owned info, products & services

Google’s ~75% share of users, ~90% of publishers/advertisers

Publicly Inaccessible

Black Box: Metadata, Algorithm, Auction Quality Score

“King Maker” Inside Knowledge:

Hidden Search Biases/Conflicts
Detailed Profiles of All User Types
Near Perfect Knowledge of:
Traffic, Supply & Demand,
Relationships, Locations, & Intent

Omni-tracking of users, publishers, advertisers is publicly inaccessible

Google favors Google’s free info, products & services in its search rankings

Google favors Google-owned free content verticals in Google’s search rankings

Google sees out, but no one sees in

Google’s information ranked according to Google’s biases/conflicts

Calendar, Docs, Gmail, Groups, Knol, Orkut, Picassa, Reader, Talk, Translate, TV, Voice, YouTube, Mobile

World discovers Google info/products/services first/easiest

Google Buries Rank of: TradeComet, MyTriggers, Foundem, Ciao, Ejustice.fr, Navx...

9/13/2010

Scott Cleland -- Precursor LLC
Googleopoly’s Secret Weapon

Google’s “Innovation Without Permission” is Code for:

Unfettered “Deep Tracking Inspection” or “Total Information Awareness Power”

“We can suggest what you should do next, what you care about. Imagine: We know where you are, we know what you like.”... “You can literally know everything.” Google CEO Schmidt 9-8-10

Deep Tracking Inspection – of everything that passes through Google’s cloud

• What virtually no one appreciates except Google is that the Internet is the ultimate deep tracking inspection and surveillance technology – when sent through Google’s dominant Internet media platform of data centers that copy, store and analyze most all Internet activity.
  – Everything, literally everything that is on the Internet, is ones and zeroes that by design are sent back to Google’s cloud data centers for processing, recording, storage and analysis – the only entity in the world with the mission and capability to do so.

• Other things that virtually no one appreciates except Google is:
  – What Google’s mantra “innovation without permission” means is that Google has to ask no one for their permission to use the derivative tracking metadata from anyone: publisher “partners,” advertiser clients, competitors, proprietary owners, or users -- because if the ones and zeroes pass through Google’s data centers to be processed and recorded – Google views those ones and zeroes as fair game to use in any way they see fit, because it is Google’s self-asserted, universal property right to “innovate without permission.”
    • In practical terms, innovation without permission means unfettered “fair use,” “mash-up,” “re-mix,” “open source,” and 2.0 transparency (i.e. “publicacy, the opposite of privacy).
  – What Google can reverse-engineer from all the ones and zeroes (or metadata -- data about data) that pass through Google’s data centers?
    • Google can aggregate the user and advertiser audience demographic profile of every publisher and their content down to a page, so that it could create supra-competitive content, products and services that would have the unique inherent advantage of being able to replicate the best of what everyone else does and knows.

• Google’s unique deep tracking inspection capability creates “Total Information Awareness Power” where Google can’t lose because it can use/build upon the secrets, property, and trailblazing success of everyone else -- without permission.
  – It would be like before a football season, one team had access to a copy of every opponents’ scouting reports, playbooks, game plans and signals – because they owned the league/platform that everyone else used to compete.
What are Google’s Topical Monopolization Issues?

• **Pending Antitrust Suits Against Google:**
  – US: TradeComet & MyTriggers;
  – EU: Foudem, Navx, EJustice, Ciao

• **Yahoo-Japan/Google Search/Ad Outsourcing Agreement:**
  – Grants Google 90+% of Japan’s searches; increases Google’s world search share from ~70% to ~74%; eliminates search competition.

• **Google Book Settlement (GBS):**
  – DOJ opposes GBS: as it would “grant Google sweeping control over digital commercialization of millions and millions of books;” and “good intentions of members of a price-fixing combination are no legal justification for lessening price competition.” (Per DOJ)

• **ITA Travel Software Acquisition:**
  – Expedia Chairman Barry Diller: “I think it is disturbing that Google is moving into serving individual spaces, rather than being search neutral,”... “It is a dangerous step because it is inevitably going to cause problems with customers...” (per FT)
  – Greenlight COO Pourus: Google has become the “ultimate informational intermediary;” All intermediaries “should now be rethinking their business models.” (per Comm Daily)

• **Metaweb Acquisition:**
  – Google’s acquiring MetaWeb, the leading semantic web database of more than 12 million “things;” it was probably the most critical building block for a potential search competitor to compete with, and differentiate from, Google search; while the raw database will be open and accessible to the public, only Google will collect and know the who, when, where & how semantic information is used.

• **Zynga Games Investment by Google:**
  – Online games like Zynga’s provide ~30% of traffic to FaceBook and social media and represent a substantial portion of their monetization potential; Google is co-investing with Yahoo-Japan owner SoftBank, which appears to be a possible quid pro quo reward to SoftBank for choosing Google for Yahoo-Japan’s search.
V. GOOGLEOPOLY’S DEFLATIONARY IMPACT ON ECONOMIC RECOVERY
How Google Plays the Leading Role in the Internet Deflationary Spiral

- “Internet distribution does not work if it is built on the economics of scarcity, but only works with ubiquity and abundance economics,” Google CEO Schmidt told the Newspaper Association, April 9th 2009.
  - “Ubiquity” is code for Google’s mission to make all the world’s information accessible for free.
  - “Abundance economics,” per Wikipedia, is “post-scarcity” which “describes a hypothetical form of economy or society, often explored in science fiction, in which things such as goods, services and information are free, or practically free. This would be due to an abundance of fundamental resources (matter, energy and intelligence), in conjunction with sophisticated automated systems…” i.e. Googleopoly’s Internet platform of today.

- Chris Anderson, Author of “Free – The Future of a Radical Price” said: Google’s chief economist Hal Varian “taught me everything I know about free;” “Google...is the citadel of free;” and “Google is the poster child of making money around free.”

- Only Google has the audience, business model and capability that can thrive long term on free content, products and services.
- Google increasingly is the Internet and is systematically monopolizing Internet media via the ultimate price deflation of... free.
  - Google provides search for free to over 600m users daily and over a billion users weekly, and monetizes free search, and all Google’s free products and services, with its DOJ-determined monopoly in search advertising.
  - Google, via acquisition of dominant YouTube, DoubleClick and AdMob, now has a monopoly in free IP-video distribution.
  - Google also offers most every major type of Internet product and service for free or near free -- supported by advertising.
  - Google digitized 12 million books without the permission of copyright holders and makes them available to search for free; (authors and publishers have sued Google for copyright infringement and then settled for about $10 a book. The DOJ opposes the settlement as a violation of copyright and antitrust laws).
  - Google-YouTube assumed copyrighted video should be free: “There is no question that YouTube and Google are continuing to take the fruit of our efforts without permission and destroying enormous value in the process. This is value that rightfully belongs to the writers, directors and talent who create it and companies like Viacom that have invested to make possible this innovation and creativity.” per Viacom’s press release.

- Déjà vu:
  - People get the deflationary spiral, property devaluation and job losses free Napster-ization caused the music industry.
  - People understand the deflationary spiral, property devaluation and job losses that free “Google News” aggregation of all 25,000 news sources, and free classified ads from Google satellite Craigslist caused the newspaper/journalism industry.
How Google Has a Deflationary Impact on the Economic Recovery
Internet-Related Distribution Is an At-Risk Trillion-Dollar Sector Employing Millions

“The brutal economic answer is that the Internet does in fact change other people’s businesses because of this massive distribution…” “We should just acknowledge that and not hide from it.” Google CEO Schmidt 6-21-09

• There’s no net economic growth, job creation or property value creation in a “free” Internet sector model, only: a deflationary price spiral; net negative growth, property devaluation, job losses, and monopolization.
• The “Google Economic Effect:”
  – Deflates the price for information, products and services to free -- so only targeted advertising can succeed;
  – Eliminates competition-driven: quality, diversity of choice, and innovation;
  – Centralizes/concentrates Internet distribution, which makes the economy highly vulnerable to systemic disruption.
  – Reduces employment because Google views people as inherently inefficient relative to Internet automation, and because Google views customer service personnel as unnecessary, and most sales and marketing personnel as redundant.
  – Obsoletes several hundreds of thousands of jobs rapidly -- much more quickly than the deflated Internet sector can absorb.
• Google is an unstable and unpredictable business platform for others to build businesses on.
  – While Google’s ~$25b ad “auction” platform is efficient for Google, it is not a stable economic platform/foundation on which other companies can predictably grow and thrive.
  – Google’s Internet economy is an opaque, unaccountable, intellectual-property/privacy-unfriendly, “black box” where the foundation of ranking quality scores and search/auction algorithms are constantly shifting sands.
  – Google’s CEO went so far to tell a gathering of magazine publishers in October of 2009 that: “We don’t actually want you to be successful. The company’s algorithms are trying to find the most relevant search results, after all, not the sites that best game the system.” In other words, Google views efforts by web publishers to compete and improve their search ranking as -- spam and manipulation – not normal competition! Simply, only Google is allowed to influence what information is ranked high.
• Google also has grossly overstated its economic impact publicly.
  – Google has double and triple counted its economic impact; it has not subtracted their consumption from their production to reach a net economic contribution figure; and it has completely ignored vast Google-generated negative externalities, including: the price deflation of free, job losses, and massive Google cost-shifting to individuals, suppliers and government.
What Are the Industries/Companies in Googleopoly’s Deflationary Path?

>200 info-distribution companies are at risk of being annexed, controlled, subjugated or commoditized by Google

"Our model is just better. Based on that, we should have 100% share." Google CEO Schmidt 12-10-09
VI. CONCLUSIONS & RECOMMENDATION
Why Are the Stakes So High?
What’s at risk from a global monopoly bottleneck over how most access, use and monetize the world’s information?
How are Consumers Harmed by Innovation & Free Products/Services?

- **Google’s core antitrust defense is: where is the harm to consumers from all Google’s innovation and free products and services?**
  - Essentially Google argues that Google-led innovation and free subsidized products and services are superior to, and more consumer-beneficial than, all competitors’ offerings and hence Google is better than a competitive market.
  - Unfortunately that is more an argument against competition and antitrust law than antitrust enforcement.
  - The fundamental premise of antitrust law and over a century of experience rejects this Google-is an-exception argument and maintains that competition serves consumers better over the long run than monopoly, because in the absence of competition the monopoly does not have any economic incentive to serve users interests.
  - This is especially true for Google’s which does not work for users, but advertisers.

- **How is the consumer harmed from more Google innovation?**
  - The crux here is not whether any one else will be able to freely innovate or whether there will be Google “mono-vation,” which is heavily skewed toward “innovation” that subscribes to Google's assumptions of: “innovation without permission,” which assumes hostility to the property rights of publishers, privacy rights of users, and proprietary rights of competitors. Moreover, the business model must be advertising based not subscription or micropayment; and speed and efficiency trump privacy and security in design.

- **How is the consumer harmed from free Google products & services?**
  - The crux here is not whether consumers benefit from the free product or service being offered, but whether or not the system will remain competitive so that other products and services critical to a competitive ecosystem, like accountability measurement, remain competitive and hence independent.
  - Undercutting paid-for products or services with ones that are free (based on advertising or cross-subsidization) can harm consumer by defunding consumer value and protection: i.e. responsive customer service, and privacy/security protections.
  - Free, one-sided analytics products and services that are owned by Google and not independent mean that Google can rig the competitive game by being a player that owns the referee and scorekeeper, so that future products and services need not operate in the interests of users.

- **How is the consumer harmed by free Google information?**
  - While the consumer benefits from the availability of free information, the consumer does not benefit from a monopoly system that reduces the incentive and opportunity to reap a significant reward for the creation of valuable content and that reduces the quality and diversity of information being produced going forward.
Recommendation

DOJ Should File a Sherman Section 2 Monopolization Case
EU Should File Section 102 Statements of Objections

• Google is the dominant platform for Internet media and is monopolizing the consumer Internet media ecosystem and predatorily deflating prices sector-wide—so the antitrust problem is broad & systemic, not narrow & specific.
  – To try and address the Google antitrust problem narrowly and reactively via narrow issues like the Google Book Settlement or the ITA Software transaction would be a futile antitrust game of “whack-a-mole.”
• Moreover, Google’s antitrust defenses are macro and not specific: “competition is but a click away;” Google is innovative and antitrust enforcement would impede innovation; and free products and services can’t harm consumers.
  – A Sherman Section 1 & 2 monopolization case and/or an EU Section 102 Statement of Objections are necessary to address and encompass the breadth and depth of the long term threat to Internet media and distribution competition, quality, diverse choice of information/distribution, and diverse and competition-driven innovation.
APPENDIX A: SCOTT CLELAND BIO
APPENDIX B: GOOGLEOPOLOGY RESEARCH
Appendix A: Bio: Scott Cleland, President, Precursor® LLC

- **Bio:** Scott Cleland is a prescient analyst with a long track record of industry firsts. Cleland is President of Precursor® LLC, which consults for Fortune 500 clients; authors the “widely-read” PrecursorBlog.com; publishes GoogleMonitor.com & Googleopoly.net; and serves as Chairman of NetCompetition.org®, a pro-competition e-forum supported by broadband interests. Eight different Congressional subcommittees have sought Cleland’s expert testimony on a wide range of complex emerging issues related to competition; and *Institutional Investor* twice ranked him as the top independent telecom analyst in the U.S. Cleland has been profiled in *Fortune, National Journal, Barrons, WSJ’s Smart Money, Investors Business Daily*, and *Washington Business Journal*.
  - Cleland’s Full Biography can be found at: [http://www.precuror.com/bio_long.htm](http://www.precuror.com/bio_long.htm)

- **Scott Cleland is Publisher of:**
  - [www.PrecursorBlog.com](http://www.precursorblog.com)
  - [www.GoogleMonitor.com](http://www.googlemonitor.com)
  - [www.Googleopoly.net](http://www.googleopoly.net)

- **Scott Cleland’s Congressional Testimony on Google:**
  - Before the Senate Judiciary Subcommittee on Antitrust on the Google-DoubleClick Merger, September 27, 2007. [http://googleopoly.net/cleland_testimony_092707.pdf](http://googleopoly.net/cleland_testimony_092707.pdf)

- **Presenting at the Federalist Society: Why Google is a Monopoly**
  - [http://www.precursorblog.com/content/why-google-a-monopoly-presenting-case-federalist-society](http://www.precursorblog.com/content/why-google-a-monopoly-presenting-case-federalist-society)
Appendix B: www.Googleopoly.net Research

Googleopoly Research Series:
- Googleopoly I: The Google-DoubleClick Anti-competitive Case
  - http://googleopoly.net/merger.html
- Googleopoly II: Google’s Predatory Playbook to Thwart Competition
  - http://googleopoly.net/googleopoly_2.pdf
- Googleopoly III: Dependency: The Crux of the Google-Yahoo Ad Agreement Problem
  - http://googleopoly.net/googleopoly_3_dependency.pdf
- Googleopoly IV: How Google Extends its Search Monopoly to Monopsony Control over Digital Information
  - http://googleopoly.net/Googleopoly_IV_The_Googleopacity_Case.pdf
  - Chart: Google’s Digital Information Distribution Bottleneck
- Googleopoly V: Why the FTC Should Block Google-AdMob
  - Chart: Google-AdMob Monopoly Bottleneck Chart
    - http://googleopoly.net/merger_to_monopoly.pdf

Additional Googleopoly Related Research:
- Google: “We’re the Biggest King Maker on This Earth”
  - http://precursorblog.com/content/google-were-biggest-kingmaker-earth-googleopoly-update
- What Private Information Google Collects
- Why Privacy is an Antitrust Issue and Google is its Poster Child
- Google’s “Total Information Awareness Power” – A One-page Graphic on All the Information Google Has
  - http://www.precursorblog.com/content/googles-total-information-awareness-power-a-one-page-graphic-all-information-google-has
- Googleopolyization Through Anti-competitive Search Discrimination Chart

Please visit www.GoogleMonitor.com for additional information.
TRAFFIC REPORT:
HOW GOOGLE IS SQUEEZING OUT
COMPETITORS AND MUSCLING
INTO NEW MARKETS

A Study by INSIDE GOOGLE
JUNE 2, 2010
Executive Summary

Google has been muscling into new web markets and greatly expanding its dominance of other web commerce sectors since 2007, when the web search giant adopted a controversial new business practice aimed at steering Internet searchers to its own services.

Google's dramatic gains are revealed by an analysis of internet traffic data for more than 100 popular websites. Once upon a time, these sites primarily benefited from Google. Now, they must also compete with it. In the most comprehensive study of its kind to date, INSIDE GOOGLE obtained three years of traffic data from the respected web metrics firm Experian Hitwise, allowing an analysis of Google's business practices and performance that is unprecedented in scope.

The data shows that Google has established a Microsoft-like monopoly in some key areas of the web. In video, Google has nearly doubled its market share to almost 80%. That is the legal definition of a monopoly, according to the federal courts, which have held that a firm achieves "monopoly power" when it gains between 70% and 80% of a market.¹

The report examines whether Google has erected "barriers to entry" in markets such as video by manipulating its search results so that users are directed primarily or exclusively toward Google's own services, such as YouTube.

Google's dominance in video and its huge gains in other markets such as local search and comparison shopping correlates with these increasing efforts by Google to promote its own services within search results. This

¹ http://www.justice.gov/atr/public/reports/236681_chapter2.htm#N_23
practice, which amounts to a new business model, appears to be an abandonment of Google’s pledge to provide neutral search capability.

The most striking example of how this practice enables Google to muscle its way into new markets is the lucrative market for local search. Google now inserts results from Google Maps into the first page of results from most Google searches, driving enormous traffic toward Google Maps and away from competitors. Google now has more than half the market for local search.

The ultimate significance of these developments is that they spell a rapid decline in choice for consumers. Increasingly, consumers who use Google are placing themselves in a sort of virtual gated community, or what was once known as "a company town." You can go anywhere you like, as long as you use the company’s roads. And you can buy anything you like, as long as you shop at the company’s stores.
A strategy by Google to insert links from its proprietary shopping, map and video sites into the main "results" page after a search appears to have had a steroidal effect on the company's web traffic, fueling the company's breakneck growth in ad revenues.

The Google practice, known as Universal Search, is already the subject of a complaint to the Federal Communications Commission by one British shopping-comparison website which claims Google improperly used Universal Search to depress its web traffic and steer users to a less-popular Google shopping site.

While a fair case can be made that Google's offerings in maps, video, shopping and other areas are as good or better than competitors', modest differences in quality do not appear to account for such radical and rapid shifts in traffic.

Among the biggest losers from Google's adoption of Universal Search is MapQuest, the venerable web site for maps and local directions, which has seen its traffic cut nearly in half since Google launched an assault on its franchise in 2007 using Universal Search, according to three years of data from the respected analytical firm Experian Hitwise.

In the same three-year period, the Hitwise data also shows, Google's YouTube has also nearly doubled its share of the video market from a little over 40% to more than 80% -- meeting the legal criteria for a monopoly. The site Photobucket, which once had nearly 20% of the video market, now has less than 3%. MySpace, another one-time contender with over 12% of video in 2007, now has less than 1%. Even ESPN has taken a thrashing from 8% to 4%.

Google is also rapidly clearing the field in still images, with its onetime main rival Photobucket going from over 31% in June of 2007 to barely
over 10% last month. Another one-time contender, Yahoo Images, has gone from over 12% to a bit over 7%. All of Google’s competitors in image searches now have less than 10% market share, according to Hitwise. Google's own market share soared from a low of 43% in mid-2007 to over 60% last year before falling back toward the mid-50% range. Flickr, another popular site, now has less than 9%.

The Importance of Local Search

The most striking example of the power of the Universal Search strategy for Google is MapQuest, a unit of AOL which now has only 32% of the market, down from 57.24% in July 2007. The Hitwise data shows that the stark decline in visits to MapQuest was accompanied by a closely matching rise in visits to Google Maps, as Google put its own service atop all others for generic address searches. MapQuest, a unit of AOL, appears likely to soon be reduced from a dominant player in web commerce to an also-ran, due in large part to the steps taken by Google to favor its own locator service. Google is now the dominant provider of local search information with more than 51% of the market. MapQuest officials declined to comment for this report.

The decline of MapQuest is likely to have a big impact -- not just in e-commerce but on the larger economy. While most people think of map sites as simply a source of driving directions, they're most often used in connection with shopping trips. With the paper-based yellow and white pages dying off, most consumers now use Internet search engines to decide where to shop near their homes.²

² On May 9, the New York Times reported that Verizon is seeking to halt distribution of paper white pages directories in New York State. http://www.nytimes.com/2010/05/08/nyregion/08verizon.html?src=me
That makes local search one of the most lucrative corners of the Internet, and also gives one company -- Google -- enormous power over the bricks-and-mortar economy. While e-commerce has become a substantial economic force, the reality is that people still do most of their shopping in stores near their homes. If Google comes to dominate local search the way it dominates other areas such as video, a day may not be far off where
small businesses feel they have no choice but to engage with Google. And consumers would end up being steered, many without their knowledge, toward the local businesses that are willing to participate with Google.

As the Department of Justice and the Federal Trade Commission eye Google for possible antitrust violations, the question of whether the Mountain View search giant uses its dominant position in search to muscle its way into other businesses is vitally important.

Under the definitions of U.S. antitrust law, Google already has "market dominance" in search and search advertising with over 70% of the market, much as Microsoft has market dominance for computer operating systems. That means Google, like Microsoft, could get into trouble by "bundling" its dominant product with other services as a way to seize new markets.3

The rise of Google Maps has also hammered MapQuest's once-formidable competitor, Yahoo Maps, the Hitwise data shows. Once the market leader with about 41% of traffic in 2005, according to Hitwise, by April of 2007, Yahoo had ceded about half its traffic to Google and has now slid to just 6% of the market. Microsoft's Bing has about 4.5%.

Google can certainly argue that it provides a better user experience than MapQuest or Yahoo for local search and mapping. Yet there is little question that Google's rapid ascent in local search and mapping is due less to consumer preference than to the Universal Search strategy it adopted in 2007. Universal Search shoehorns maps and relevant local hits directly into the results produced by Google's famed search algorithms.

"The ascent of Google Maps is a result of the shortcut in the search results on Google," Heather Hopkins of Hitwise determined in a blog post in

---

3 See http://www.readwriteweb.com/archives/the_anti-trust_case_that_could_be_in_the_works_agpa.php and http://www.wired.com/techbiz/it/magazine/17-08/mf_googloopoly
February of 2009. "61% of visits to Google Maps came directly from Google last week."4

Hopkins also reported that MapQuest "receives most of its search traffic from searches for its brand name - in other words from people actively searching for MapQuest." In the period she examined, about 80 percent of search queries that ended up sending a user to MapQuest were for the MapQuest name. Contrast that with Google, where only 4% of the site's search traffic came from people searching for "Google Maps" or similar branded terms.

When Universal Search was launched in 2007 it applied to Images, Maps, Books, Video, and News. "The ultimate goal of Universal Search is to break down the silos of information that exist on the web and provide the very best answer every time a user enters a query," Google vice president Marissa Mayer explained at the time.5 The "best answer" will appear in "a single set of blended search results," Mayer said.

Contradictorily, Google continues to maintain that its search results are neutral. Said the company in its 2007 announcement:

"As always, Google™ search results are ranked automatically by algorithms to deliver the best results to users anywhere in the world."

It is hard to see how this can still be true, given the increasingly pronounced tilt toward its own services in Google's search results.

_________________________

Images Also Shows Big Gains

In images, Google has now opened up a gaping lead with about 55% of the market and everyone else down around 10%. Google's image numbers are inversely related to those of Photobucket, suggesting that the search engine is being used to draw traffic away in a manner similar to what is happening to MapQuest.
Video Killed the Hollywood Stars?

In terms of hard numbers and slanted lines, nothing is more graphic than Google's increasing dominance of video, where YouTube's traffic has nearly doubled in just three years to about 80 percent of the market -- while all of its competitors now languish in the single digits. Again, it is hard to account for such crushing market power simply by branding or quality, given that Google Video is up against some of the world's biggest and best-financed brands such as Fox and Disney.
Shopping Comparison: The Foundem Case

Another striking example of the market power of Universal Search is shopping price comparison websites. As documented by the British company Foundem in a submission to the Federal Communications Commission, Google's product search service has virtually annihilated several once-popular shopping-comparison sites since it was integrated into Universal Search in December 2007.⁶

In November 2007, Google product search had about 1.3 million unique visitors. The next month, that figure shot up to 11.9 million. By December of 2009, Google product search had more than 20 million unique visitors, making it second only to Shopzilla with 21 million, a gain of more than 1200%.


⁶ [http://www.foundem.co.uk/FCC_Comments.pdf](http://www.foundem.co.uk/FCC_Comments.pdf)
Universal Search: How Powerful Is it?

Google still has formidable rivals in some online marketplaces and the impact of universal search in such cases is not always so easy to discern. In both books and news, competition remains fierce. Yahoo remains the leader in news with about 23% of the market and Google is far behind with only about 7%, Hitwise data shows. In books, Google lags far behind Amazon and is also slightly behind Barnes & Noble. What is unknowable is whether Google will choose to juice its market share in the future by making additional changes in Universal Search that favor its own book and news products. Google has already announced it will begin selling books as early as next month.

Universal Search makes rubbish of the notion that Google's search results are strictly neutral based on some secret recipe. The company is nonetheless moving increasingly toward this strategy of deliberately manipulating search results. Recently, Google rolled out a new look to its results page which takes another step toward pointing users to its own services by adding a permanent left-hand side navigation bar.

Here's how it works. Say you are researching the Mark Twain character Tom Sawyer. Put that name into the primary search box and you'll get a Wikipedia entry, a hit on Sparknotes, and then results from Google Images, YouTube, and Google Books -- all components of Universal Search. That takes up most of the first page, although if you scroll down far enough you eventually get to an Amazon hit. Then, if you click the "Books" tab at left, you get dozens of results only from Google Books -- even though there's nothing to indicate that by searching "books" you have been corralled into a proprietary and exclusive service of Google featuring only Google products. (Curiously, video search does not seem to be a gated community, at least not yet. Searching Tom
Sawyer in video gives you five YouTube results first, then options from Amazon, Yahoo, and others.) See how it works in the illustration below:
The results are even more striking when the search is explicitly related to a popular consumer good. Search for "organic coffee," and you're likely to get a screen dominated by Google Shopping results, Google Local Search results, a Google Checkout hit, and numerous paid ads.

The impact of Universal Search has received notice primarily among the cognoscenti of the search engine community, where one insider blog, SEOBook.com, lampooned the strategy.
http://www.seobook.com/google-universal-search

Only a few of the Internet's more astute observers have picked up on how it changes the dynamic of competition in e-commerce.

Shortly after the rollout of Universal Search, web commerce guru John Battelle noted in 2008 that "Google is becoming more and more of a media company in the traditional sense in that it is driving traffic to properties it already owns.

"And whether or not it does so with transparency, and whether or not we believe that it truly is the best place to end up -- on their maps as opposed to MapQuest or whatever -- the truth is that the interface that's being created, this sort of one-box, universal blended interface that's starting to appear on Google is forcing a
renegotiation of the relationship between content owners and Google."

Universal Search, concluded Battelle, is taking Google across an invisible line in the marketplace from a neutral purveyor of choices to an agent which preselects choices. "Where we used to think [Google] was great because it was just a link and they drove us a bunch of traffic and we could trust them to pick the best link, now we are competing with Google on properties."7

Ironically, Google's competitors Yahoo and Bing have also been adopting the idea of Universal Search as a way to enhance their results and prop up properties such as Yahoo Maps, and many commentators say Google is simply responding to competition with its new approach.

But it appears that Google has been after this result for a long time. Google engineers filed their first patent for a Universal Search process on Dec. 31, 2003.8

One of the names on that patent is Marissa Mayer, Google's vice president of Search Product & User Experience, who dates the quest back even further in a 2007 blog:

Back in 2001, Eric [Schmitt] asked for a brainstorm of a few "splashy" ideas in search. A designer and product manager at the time, I made a

7 http://www.youtube.com/watch?v=zy-9ZzRk3Lo

few mockups -- one of which was for 'Universal Search.' It was a sample search results page for Britney Spears that, in addition to web results, also had news, images, and groups results right on the same page. Even then, we could see that people could easily become overwhelmed with the number of different search tools available on Google -- let alone those that would be created over the next few years. This proliferation of tools, while useful, has outgrown the old model of search. We want to help you find the very best answer, even if you don't know where to look.

That mockup and early observations were the motivation behind the Universal Search effort we announced earlier today.⁹

Mayer paints the Universal Search project in the sort of humanitarian, semi-Orwellian language that regularly comes out of Mountain View.

"With Universal Search, we're attempting to break down the walls that traditionally separated our various search properties and integrate the vast amounts of information available into one simple set of search results," she writes. "We want to help you find the very best answer, even if you don't know where to look."

The reality is a bit more crass: Universal Search now populates the top of the results page mainly with results from Google's own product lines. These changes bring the search giant several steps closer to a closed ecosystem where real consumer choice no longer exists.