Privacy in the Age of Big Data

The Players, Regulators, and Stakeholders

Chapter 1: The Perfect Storm

If, like us, you spent the last 20 years or so working in the high tech industry, you've had a bird's-eye view of the evolving data privacy debate. No matter where you fall on the privacy continuum—from a cavalier approach to how your data is being collected and used to a more cynical and, some might argue, paranoid view of the endless ways your information could be hijacked—it is safe to say that the stakes have never been higher.

There is a perfect storm brewing. A storm fueled by innovations that altered how we talk and communicate with each other. Who could have predicted 20 years ago that the Internet would have an all-encompassing effect on our lives? Outside of sleeping, we are connected to the Web 24/7, using our laptops, phones, or iPads to check our email, read our favorite blogs, look for restaurants and jobs, read our friends' Facebook walls, buy a book, transfer money, get directions, tweet and foursquare our location, or organize protests against dictatorships from anywhere in the world. Welcome to the digital age.

Digital technology has created and nurtured a new world order where much that was impossible is now possible. We may not have personal jet packs or flying cars, but we do have video phones and combat drones. We may not yet inhabit the world George Orwell predicted in his dystopian novel, *1984*, a world in which there was no right to privacy and the government used surveillance and misinformation to control its citizens; however, our government has certainly used our personal information to its advantage, resulting in far more knowledge about us than even Orwell could have imagined.

Our world has changed; some might argue for the better and others for the worse. Today, we give away more information about ourselves and have more data collected and aggregated about us than any group in human history. Most of it we give away for simple convenience and the use of "free" or almost free services. Some of it is collected surreptitiously or through aggressive government action, such as the eight million requests the U.S. Department of Justice made to Sprint in 2009 for subscriber locations via their GPS phones.

Our offline life is now online. We trade our personal information for online conveniences like ecommerce, instant communication, keeping in touch with hundreds of friends or business colleagues, networking with communities about things we care about, and even for the chance of romance. In exchange, we are marketed to. Our data is aggregated and segmented in all sorts of ways: by age, by sex, by income, by state or city or town, by likes, by sites we visit. We are grouped in terms of our behavior and these groups are "rented" to advertisers who want to sell us things.

Much of the privacy debate is centered around, or so most pundits will tell you, behavioral targeting. In a recent study conducted by U.C. Berkeley and the University of Pennsylvania, 66 percent of those surveyed said they did not want marketers to tailor advertisements to their interests. When participants were told how their activities were tracked, the disapproval rate climbed higher, to between 73 and 86 percent. In a recent survey by Opera Software, Americans said they were more fearful of online privacy violations than they were of terrorist attacks, personal bankruptcy, or home invasions.

The concept of targeted advertising is not new. Yes, today it is much easier to digitally track everything, sort through it, and make educated guesses about what we'll buy. But is more intrusive advertising something to be feared? It is when you consider that this same process can be used to make educated guesses about a wide range of activities. Security agencies can use it to profile possible terrorists, the IRS to identify possible fraudulent tax returns, law enforcement agencies to surveil possible criminal activities, credit card and loan companies to determine good and bad credit risks. While data, in itself, may be benign, how it is used can run the gamut from harmless to what some might call exceedingly harmful and others might call truly evil.

Data privacy is not a debate about how we are advertised to. It is a debate about the collection and use of our personal information from a commercial and political standpoint. By giving out our information for the convenience of products and services, we have also opened the door to far more intrusive monitoring by government agencies in the name of national, state, and local security. How we reached this point is the result of technological innovation and entrepreneurship. Where we go from here is up to us.

Through the Looking Glass

It all started in 1969, with the founding of ARPANET (Advanced Research Projects Agency Network), a network of geographically distributed computers designed to protect the flow of information between military installations. This laid the groundwork for the Internet, a network of networks and now home to millions of private, public, government, business, and academic networks all linked together and carrying vast amounts of digital information.

Along the way, several inflection points occurred that would end up putting the Internet at the center of our professional and personal lives:

- **The Internet becomes a household word.** In 1990, Sir Tim Berners-Lee wrote the initial specification for the World Wide Web, and by 1993, Digital Equipment Corporation (later acquired by Compaq) officially "opened" its first commercial website. The mid-1990s featured the introduction of web browsers and heralded increasing access to PCs, with two out of three employees and one in three households having access.

- **Shopping goes online.** eBay and Amazon got their start in 1995 with a new business model directed solely at the online consumer. This set the stage for traditional brick and mortar businesses recasting themselves in the online world, as well as the emergence of new online-only businesses like Zappos and Netflix.

- **Search goes mainstream and validates a powerful, new advertising model.** In 1998, Google, following search pioneers like Yahoo and Lycos, went live with a better search algorithm, as well as superior ad targeting mechanisms. This not only changed the way anyone searched for information, but perfected **content-ba**sed and paid query-based advertising models that resulted in Google's $8.44 billion in revenue in the fourth quarter of 2010 alone. It also produced the largest collection of data on individual behavior in history.

- **Social media takes off.** In 2003, following struggling social network pioneer Friendster (now a social gaming site), MySpace went live and grew to become the most popular social network until Facebook overtook it. In 2004, the term social media was coined (first used by Chris Sharpley) and Facebook was launched. In 2005, YouTube goes online, followed by Twitter in 2006. All of these sites (and more) produce vast amounts of digital data on individual behavior, the relationships between people (the idea of the personal social network) as well as their location (from services like Foursquare).

- **The rise of personal devices.** In 1996, the Nokia 9000 Communicator becomes the first mobile phone with Internet connectivity. In 2001, Blackberry is launched, the first email-enabled mobile phone system. In 2007, Apple introduces the iPhone, which sets the stage for a host of mobile web applications and businesses. By 2008, there are more mobile phones with Internet access than PCs. In 2010, tablet devices, led by the iPad, take the market by storm, with more applications churning out more data. For the first time, a user's location is an integral component of the device itself. It is now possible to know where someone is located at any time without them telling you.

- **Communication becomes instant**. AOL's Instant Messenger (IM) introduced real-time messaging in 1996, which reached a much broader personal and business audience with the introduction of Skype and Microsoft's MSN Messenger. The SMS (Short Message Service) protocol was developed in 1984, making it possible for mobile devices to also send text messages; this is now the preferred method of communication for teenagers and young adults. It is estimated that there will be over 3.4 billion IM accounts by 2014. Similar to social media sites, instant messages produce vast amounts of information, not only about individual users but also about the depth and quality of their relationships with other people and organizations—the all-important social graph.

Today, we operate in an always-on, digital world: we work online, we socialize online, we follow news and our favorite shows online, we file taxes online, we bank online, we may even gamble or pursue sexual interests online. And everything we do leaves a digital footprint, so much so that we had to give it a name: big data.

Welcome to the Big Data Age

Unless you've been asleep for the past few years, you've probably read about the amount of data generated by our digital universe. Phrases like "drowning in data," a "vast ocean of data," "exponential data growth," have been invoked to try to capture its size. Why? Because it's almost too big to grasp, or as IDC Research put it:

- In 2009, the digital universe grew 62 percent or almost 800,000 petabytes (think of each petabyte as a million gigabytes, which translates into a stack of DVDs reaching from the Earth to the moon and back).
- In 2010, it was projected to grow to 1.2 million (final counts are not in as of yet) petabytes.
- By 2020, it is projected to be 44 times as big as it was in 2009 (those DVDs would be stacked up halfway to Mars).

But big data is not just about size. It's about the sheer number of data sources available, its different formats, and the fact that most of it is user generated: 70% of the digital universe is actually generated by all of us through email, Facebook, Twitter, LinkedIn, Flickr, YouTube the list goes on and on. There are:

- One trillion unique URLs in Google's index and two billion Google searches every day.
- 70 million videos available on YouTube and they are viewed 100 million times on a daily basis.
- 133 million blogs.
- More than 29 billion tweets and three million are added every day.
- More than 500 million active Facebook users and they spend over 700 billion minutes per month on the site.

Add to that the growing number of publicly available data sources from federal, state, and local government agencies, academic and research institutions, geospatial data, economic data, census data; this list goes on and on as well. With all that data being digitally proliferated, maintaining one's privacy from government or commercial organizations is a difficult, if not impossible, task.

From Pieces of a Puzzle to a Complete Picture: The Future Is Now

While the amount of data about us has been increasing, so has the ability to look at and analyze it. We have gone from having little bits and pieces about us stored in lots of different places off- and online to fully formed pictures of who we are. And it is all digitally captured and stored.

Historically, the science of data-mining, predictive, and exploratory analytics had been held back by two things: the inability to store enough data and the cost of the computer power to process it. Today, the costs of storage and processing power are dropping exponentially and seem likely to continue to do so. At the same time, there is an unprecedented aggregation of data about each one of us available in digital format. This makes it easy for organizations of all sizes, as well as government agencies, to find information about any individual as well as use analytic models to predict future behavior.

Far more is known about us than ever before and that information can be used to predict behavior of all kinds, including buying, political, or criminal behavior. This same information is also routinely used to create profiles that identify potential threats to domestic or international security which, in sufficiently repressive regimes, could be fatal for citizens that match a predictive model's high-risk profile, guilty or not.

Advertising as the Big Bad Wolf

Is behavioral advertising really the big bad wolf when it comes to our privacy? Certainly, the concept is not new. It is simply a way to predict, by your behavior, what service or product you might be interested in buying.

In the pre-digital days, there were companies that specialized in analyzing buying behavior, like AC Nielsen, and companies that "rented" out their customer list, segmented by income level, sex, marital status, buying behavior, etc. Chances are your mailbox, like ours, was stuffed with all kinds of offers and you seemed to get phone calls about buying or selling something every hour. Most likely, those offers were the result of information you gave to your bank, credit card company, grocery store, or as a magazine subscription holder. But the information was, to some extent, blind. Your name and address were rented, usually as part of a group, but the renter (the business or organization that bought the advertising) did not have that information until, and unless, you responded. If you did, you then became a part of that company's mailing list and they would begin to build their own profile about you. So, even then, there were multiple profiles of you in multiple lead or customer databases based on your behavior with a specific company or organization.

In the Internet age, if my website travels indicate that I love Hawaii (targeted behavior), then I would see ads for trips to Hawaii when I am surfing, whereas someone who loves Alaska would see ads for trips to Alaska. This is simply a more personalized version of online advertising. You get served up ads based on where you go and what you do because your behavior is being tracked, and from that behavior, assumptions are being made about you. Advertisers like this model because they are able to reach a more interested audience with ads that are more relevant to them, which means that they are able to sell more stuff.

The difference between then and now is that everything you do online can be captured digitally and then analyzed and tied back to you. Google tracks online behavior, demographics, and interests with an advertising cookie. Lots of companies track your behavior—mostly through cookies that you allow, knowingly or not, to be installed on your desktop or other personal device—and there's a whole bunch of companies, like eXelate, that sell your information. But for the most part, this information does not identify you specifically. Rather, it puts you in a group of people with similar demographics and interests and that group is then "rented" to someone to advertise (online of course) to.

However, instead of multiple profiles, it is fairly easy to pull them together to get a much better understanding of who you are and what you do. For example, Spokeo aggregates publicly available information about you from phone books, social networks, marketing surveys, real estate listings, business websites, and government agencies. If you search on your name, you may be surprised to see information about precisely where you live (from Google Maps), how much you paid for your house and the property taxes for it (from government data sources), the name of your spouse (from government records), how many people live in your home (from census data), all your phone numbers (from online yellow pages), previous addresses and the cost of those homes, and depending on how public your social media presence is, far more information than you might want anyone to know outside of your close circle of family and friends. Most of this information could be gotten pre-Internet, but would have required a great deal of time and effort to visit the various agencies, fill out the forms, and then often, pay a fee. Today, all it takes is entering your name, or anyone else's, into a field and clicking Submit.

And it's not just about cookies anymore. For example, public data that might contain personal information about you can be scraped (otherwise known as web scraping), collected, and analyzed. There's also a relatively new concept, location marketing, where you are served up ads based on your location (which is available from the GPS chip in your phone). So, if your GPS location indicates that you are near a specific store, you could receive ads or coupons specific to that store.

Depending on your point of view, the amount of data that can be collected about you from public and private sources can either be disturbing or simply the price you pay for living in a digital world. After all, the sites you use—like Facebook, Twitter, LinkedIn, Google, Foursquare, fill in the blank—need a business model that ensures their lasting presence. The implicit transaction you have with any of the sites that you visit is this: for the value I receive from you, I give you something of value back. That value is your personal information and that information is rented out to advertisers on a continuous basis. And since there is so much more information about you, which makes it far easier and much more lucrative to advertise to you, your personal information is now more precious than gold.

But here's the thing: in concept, there is nothing morally wrong about behavioral advertising as long as you, the consumer, are aware of it. If your personal data is collected and used solely for the purpose of advertising, its impact is pretty benign. What is not so benign is the other ways that same data can be used. The privacy debate isn't about behavioral advertising, it's about all the other ways in which your data can be mined and used. If we, as consumers, continue to associate data privacy with advertising practices, we are ignoring a far bigger issue: who is using our data, why are they using our data, and how can we protect ourselves from privacy invasions when we don't even know who is watching us?

Big Brother and Big Data Around the World

Governments are increasingly investing in capturing and analyzing digital footprints to combat crime and terrorism, flashpoint words guaranteed to galvanize most citizens to rank security over privacy when debating this issue. After all, how can we argue for privacy if our way of life is at risk?

The United Kingdom uses digital video technology to track citizens and visitors. They have more than 1.85 million CCTV cameras installed, or one camera for every 32 people. Any person walking across London will be captured on camera hundreds of times a day. British authorities have considered banning hooded sweatshirts to make this type of surveillance easier, as well as using artificial intelligence programs to identify pre-crime behavior so that officers can be dispatched before a crime is committed.

In the United States, many law enforcement agencies heavily rely on data collection and analysis techniques. New York City police would enter a person's name, physical description, ID, and companions' names into a central database when they approached people in so-called "stop and frisk" operations. In 2010, these operations, which did not require police officers to observe any criminal behavior before "stopping," were performed on over 590,000 mostly Black or Hispanic persons. However, law enforcement is no longer allowed to keep a database on individuals caught up in these blatantly discriminatory "stop and frisks" due to a state law in 2009 which makes it illegal. But the "stop and frisk" and many other databases, including a CCTV video database of individuals who have been accused of no crime, continue to play a major role in NYC's data and analytics intensive Real Time Crime Center.

Monitoring technology is taking off across the United States. CCTV cameras are installed across highway systems to monitor the flow of traffic and at traffic lights to monitor stop light violations. It is now commonplace to receive traffic citations in the mail. Although the practice remains controversial and is often challenged on constitutional grounds, it appears it's here to stay. Digital event recorders (aka black boxes in cars), similar to those on planes, are being used by law enforcement to assess fault in accidents. Rental car agencies use similar technology along with GPS recorders to assess fines for going too fast or taking a car on to dirt roads.

Depending on the circumstance, it appears that the U.S. government has differing views on the preservation of privacy in the digital age. Internationally, it sees privacy as a democratizing force. For example, the government has given grants to technology providers to ensure that social networking tools like Twitter and Facebook are secure and not easily disrupted. That way, these tools can be used more effectively by pro-democracy demonstrators in places like Syria, Tunisia, and Iran. Of course, those governments have been known to use these same tools to target enemies of the state and, during times of unrest, to cut off all access.

In matters deemed as domestic security, the U.S. government pushes for more access to personal information. For example, the U.S. Department of Justice recently argued that the continued safety and security of the United States was dependent on maintaining a clause in the misnamed Electronic Communications Privacy Act that allows warrantless searches of an individual's email if it is stored in a hosted service, such as Gmail or Hotmail, if it is older than six months old. Through the Patriot Act, law enforcement can request broad surveillance powers from a special court, which has far lower standards than those required for probable cause. Under this act, all library records for an individual can be turned over without the individual's knowledge, as the request is considered secret.

While the U.S. constitution does not specifically mention privacy, several amendments in the Bill of Rights have been held by the Supreme Court as penumbral rights of privacy. Since this is a controversial part of the law and we are not lawyers, we will stick with the safe statement that the legal definition of what is private and what is not is unclear in the "real world" but when compared to the digital one, seems crystal clear. In other words, our "right to privacy," both in the digital and non-digital world, is constantly changing. However, in the "real world" there are precedents that approach the legal standard of "settled law" (Stare Decisis) but like the technologies that drive it, there is nothing remotely settled about privacy law in the digital world.

This is the fundamental question we are faced with: in the digital age, do we have a right to not be observed by our government? If so, where: on the Internet, at the library, in public places, in private business, on the highway, or peacefully demonstrating against a government? In 1759, Benjamin Franklin said, "They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." The question of privacy versus security has always been a profoundly difficult one. But the easy access and aggregation of individuals' private digital data makes it far more complicated in this age of terrorism and weapons of mass destruction.

At the Crossroads: Privacy versus Security and Safety

In the digital age, is privacy, as Mark Zuckerberg famously suggested, outmoded? After all, if you have done nothing wrong, there's nothing to worry about. Of course, if you make that statement to anyone who has been racially or religiously profiled, you might be surprised at their reaction. We are at a crossroad: how much privacy are we willing to give up? How transparent do we want to be? How much do we want our government to watch us? How much risk, in terms of crime and terrorism, are we willing to accept as the price for our privacy? How do we measure that risk—how do we know that by giving up a certain level of privacy we are safer?

If you share photos taken from your cell phone online, chances are the embedded GPS information that precisely indicates the location at which the photo was taken went with it. Maybe it was a photo of your children at school and maybe you didn't want just anyone to know where that school was located. If you were on a community site, maybe you shared how a family member was very ill. Now you are looking for healthcare coverage and somehow that information, unknown to you, is known to the insurance company. Maybe you disabled GPS tracking on your phone so that your location would be unknown. But law enforcement can still locate you with it. Maybe you live in France, where your data is required to be stored for a year by Google, eBay, and countless other companies. The French authorities want access to it should you be investigated. Maybe you tweet. Well, now the location of your tweet can also be tracked. Maybe you are fomenting a revolution using Facebook. Maybe the government you are demonstrating against is using Facebook to watch you.

It is one thing to collect and track information with your permission. But many companies and organizations have violated that permission, assuming that you opt in so that you are forced to opt out, putting cookies on your desktop without your knowledge, using questionable practices to collect data about you, sharing your information when you've asked them not to. Technology has made snooping easy and it's difficult to keep up with what you need to do to protect yourself.

If you think that it's the government's job to protect you, think about this for a moment: in the U.S. alone there are over 30 federal statutes and over 100 state statutes that protect some aspect of privacy. The regulations are piecemeal and designed to protect you if an industry, through self-regulation, does not. There is a pending Internet Bill of Rights and a possible do not track system similar to the do not call list that governed telemarketers. There are also consumer privacy organizations and action groups and companies that have made a business out of protecting your privacy, such as TrustE. Although the Internet is global, the privacy issue is not, so privacy laws and regulatory actions and bodies differ from country to country.

We live in a complicated world. There are privacy players, regulators, and stakeholders; all holding forth on the state of privacy today and whether you should be confident or afraid about what is happening. What has become lost is exactly what our "right to privacy" means:

- What assumptions can we make about the personal data we now share online?
- Who owns our data and what are they entitled to do with it?

- What regulations are in place to protect us in the U.S. and abroad?
- What forces are at play trying to shape data privacy laws and expectations?
- What are legitimate government uses of digital data in a democracy?
- What role should we, the consumer, play in all of this?

In 1597, Sir Francis Bacon said, “Knowledge is power.” It was true then and it’s true now. The more informed we are about privacy in the age of big data, the more we can shape and affect data privacy policies, standards, and regulations. This is not a debate about advertising; it is a debate about how we balance privacy, security, and safety in an increasingly transparent and dangerous world.

Bibliography

1. Kim Zetter, "Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year," *Wired*, December 1, 2009, http://www.wired.com/threatlevel/2009/12/gps-data/

2. Cameron Chapman, "The History of the Internet in a Nutshell," Six Revisions, November 15, 2009, http://sixrevisions.com/resources/the-history-of-the-internet-in-a-nutshell/

3. Wikipedia, "Internet," http://en.wikipedia.org/wiki/Internet

4. Wikipedia, "AOL Instant Messenger," http://en.wikipedia.org/wiki/AOL_Instant_Messenger

5. Wikipedia, "SMS (Short Message Service)," http://en.wikipedia.org/wiki/SMS

6. Berkman Center for Internet and Society, Harvard University, "A History of Digital Data Creation," http://cyber.law.harvard.edu/digitaldiscovery/timeline_files/frame.htm

7. The Radicati Group, Inc., "Key Statistics for Email, Instant Messaging, Social Networking and Wireless Email," April 19, 2010, http://www.radicati.com/?p=5290

8. Pew Research Center, "Pew Internet and American Life Project, Internet Trend Data," http://www.pewinternet.org/Static-Pages/Trend-Data/Online-Activites-Total.aspx

9. Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, Michael Hennessy, "Americans Reject Tailored Advertising and Three Activities that Enable It," September 29, 2009 http://ssrn.com/abstract=1478214

10. Opera Software Press Release, "Who's Watching You," January 28, 2011, http://www.opera.com/press/releases/2011/01/28/

11. Michael Rappa, "Business Models on the Web," Managing the Digital Enterprise, January 17, 2010, http://digitalenterprise.org/models/models.html

12. Google, "Google Announces Fourth Quarter and Fiscal Year 2010 Results and Management Changes," January 20, 2011, http://investor.google.com/earnings/2010/Q4_google_earnings.html

13. IDC Research, "The Digital Universe Decade," May 2010, http://www.emc.com/collateral/demos/microsites/idc-digital-universe/iview.htm

14. NOAA (National Oceanic and Atmospheric Administration), "Tsunamis May Telegraph Their Presence," January 19, 2010, http://www.noaanews.noaa.gov/stories2010/20100119_tsunami.html

15. Adam Singer, "49 Amazing Social Media, Web 2.0, and Internet Stats," The Future Buzz, January 12, 2009, http://thefuturebuzz.com/2009/01/12/social-media-web-20-internet-numbers-stats/

16. Facebook, “Press Room Statistics” http://www.facebook.com/press/info.php?statistics

17. Nathan Wolfe, Lucky Gunasekara, and Zachary Bogue, “Crunching Digital Data Can Help the World,” CNN, February 2, 2011 http://www.cnn.com/2011/OPINION/02/02/wolfe.gunasekara.bogue.data/

18. Terri Wells, “ Website Marketing: How and Why Behavioral Advertising Works,” November 1, 2006, http://www.seochat.com/c/a/Website-Marketing-Help/How-and-Why-Behavioral-Advertising-Works/

19. Matt Drake, “Ban the Hood for Good,” EXPRESS.co.uk, March 30, 2009, http://www.express.co.uk/posts/view/39622/Ban-the-hood-for- good

20. Stuart Turton, “AI Could Power Next-gen CCTV Cameras,” PC PRO, June 25, 2008, http://www.pcpro.co.uk/news/208452/ai-could-power-next-gen-cctv-cameras

21. New York Civil Liberties Union, “NYPD Stopped Record Number of Innocent New Yorkers in 2010, New Stop-and-Frisk Numbers Show,” February 23, 2011, http://www.nyclu.org/news/nypd-stopped-record-number-of-innocent-new-yorkers-2010-new-stop-and-frisk-numbers-show

22. Michael S. Schmidt, “Have a Tattoo or Walk With a Limp? The Police May Know,” *New York Times*, February 17, 2010, http://www.nytimes.com/2010/02/18/nyregion/18tattoo.html?_r=1

23. Wikipedia, “Electronic Communications Privacy Act,” http://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act

24. Mary Minow, “The USA PATRIOT Act and Patron Privacy on Library Internet Terminals,” LLRX, February 15, 2002, http://www.llrx.com/features/usapatriotact.htm

25. Joan Starr, “Libraries and National Security: An Historical View,” First Monday, December 6, 2004, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1198/1118

26. Stanford Encyclopedia of Philosophy, “Privacy,” September 18, 2006, http://plato.stanford.edu/entries/privacy/

27. Wikipedia, “Confrontation Clause,” http://en.wikipedia.org/wiki/Confrontation_Clause

28. Wikipedia, “United States Bill of Rights,” http://en.wikipedia.org/wiki/United_States_Bill_of_Rights

29. Wikipedia, “NSA Warrentless Surveillance Controversy,” http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy

30. Wikipedia, “President’s Surveillance Program,” http://en.wikipedia.org/wiki/President%27s_Surveillance_Program

31. Unclassified Report on the President's Surveillance Program, July 10, 2009
http://www.scribd.com/doc/17267628/Unclassified-Report-on-the-Presidents-Surveillance-Program

32. USA Today, "NSA Has Massive Database of Americans' Phone Calls," May 11, 2006
http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm

33. Philadelphia Independent Media Center, "Why We Should Be VERY WORRIED about How Bradley Manning Is Being Treated," March 15, 2011
http://www.phillyimc.org/en/why-we-should-be-very-worried-about-how-bradley-manning-being-treated

34. Mobile Marketer, "Location-based Marketing Can Increase Average Order Value, Frequency, Loyalty," Dan Butcher, March 29, 2011
http://www.mobilemarketer.com/cms/news/q-and-a.html

35. Fast Company, "Google, eBay, and Facebook Take on France Over User Privacy," Austin Carr, April 5, 2011
http://www.fastcompany.com/1744794/google-ebay-facebook-take-on-france-over-privacy

36. Managing the Digital Universe, "Data Privacy," Michael Rappa, January 17, 2010
http://digitalenterprise.org/privacy/privacy.html

37. The Wall Street Journal, "Proposed Bill Would Put Curbs on Data Gathering," Julia Angwin, March 10, 2011
http://online.wsj.com/article/SB10001424052748704629104576190911145462284.html?mod=e2tw

38. ReadWriteWeb, "What Twitter's New Geolocation Makes Possible," Marshall Kirkpatrick, November 19, 2009
http://www.readwriteweb.com/archives/twitter_location_api_possible_uses.php