# Looming private information fiasco versus the new cloud business model:

The next generation will ask "***Where were you when this was going down?***"

**Carl Hewitt©2011**
http://CarlHewitt.info

**Smartphones are going to have it all: proprietary business strategies, chiseling on taxes and expenses, Roman Catholic confessions, political activities, abortions, personnel decision making, love trysts, STD, mental illness, and cancer diagnoses and treatments, *etc*.** Stored in data centers this information will have to be tightly regulated with respect to how it can be used in marketing, personnel decisions, *etc*. Government officials will become increasingly knowledgeable about the treasure-trove of intimate personal information and proprietary business information stored in data centers.

**Security officials will be forced to recognize the value of this information for preventing terrorism. Since it is politically necessary to do everything possible to prevent terrorism, means will be developed for security agencies to analyze all this information in real time**. (The recent US government WikiLeaks subpoenas and National Security Letters to Twitter and other cloud aggregators such as Facebook have heightened awareness of the threat.) **Thus we have reached an existential moment for the fate of our proprietary business and intimate personal information.** The next generation will ask "***Where were you when this was going down?***"

**A nation cannot allow its people to be able to be blackmailed or its companies' proprietary information to be taken by foreign security agencies. Before information on a person stored in a company's data centers can be turned over to a foreign government, the company will be required to first get permission from the person's country.** (Penalty to be determined.) **If necessary, a nation's intimate personal and company proprietary information will be required to be stored in data centers located in the same nation.**

Industry is undertaking a major shift in cloud computing strategy to forestall the above threat to their international business. **The alternative new cloud business model is:**

- ***perform computation using customer equipment*** because
  - it's less expensive than data center computation because of lower communications, energy, and equipment cost
  - many-core architectures will provide plenty of computing capacity, even on smartphones
  - response time can be faster than data center computation for new collaborative natural language interfaces (à la Kinect, *etc*.)
- ***store private information in data centers that can be decrypted only using the customers' private keys*** because it's cheaper and more reliable to use multiple data center storage vendors incorporated in different countries. (For efficiency, information will be cached on customer equipment.)
- ***service advertising using customer equipment*** because advertising can be better targeted on customer equipment (without violating customer private information) than data centers since customer equipment has complete information as opposed to the partial information of a data center vendor
- ***perform social computing using customer equipment*** because it can be more customizable and flexible when not restricted by vendor data centers (*e.g.* Facebook)

## Contents

## Intimate Personal and Private Business Information

Client-cloud applications and aggregators (Google, Microsoft, Facebook, etc.) make money brokering advertisements (sometimes controversially, e.g. Google under investigation for alleged breach of EU competition rules ). The better targeted the ads, the more money they make. To better target advertisements, systems need intimate private information. For example, they can use a customer's eating habits together with current state of hunger and physical location to better target restaurant ads.

Providing valuable information services for free is how systems acquire the intimate private information needed to better target advertising. For example, a smartphone can help a customer organize all their information, make purchases, and communicate with others.

According to iPhone Addictive, Survey Reveals

> *Professor Tanya Luhrmann, the Stanford anthropology professor who oversaw the survey, told the San Jose Mercury News, "One of the most striking things we saw in the interviews was just how identified people were with their iPhone. It was not so much with the object itself, but it had so much personal information that* ***it became a kind of extension of the mind and a means to have a social life. It just kind of captured part of their identity."***
>
> *Part of that identity isn't just being seen as an iPhone owner, but actually perceiving the iPhone as a part of their selves.* ***Nearly a quarter of those surveyed reported that the iPhone felt like an extension of their brain or body****.* (emphases added)

According to Google boss says 'nobody was harmed' by Buzz debacle

> *"****A phone is no longer a phone, it's your alter-ego****," he* [Google CEO Eric Schmidt] *said.* (emphasis added)

According to Google CEO Eric Schmidt Google's goal: to organize your daily life

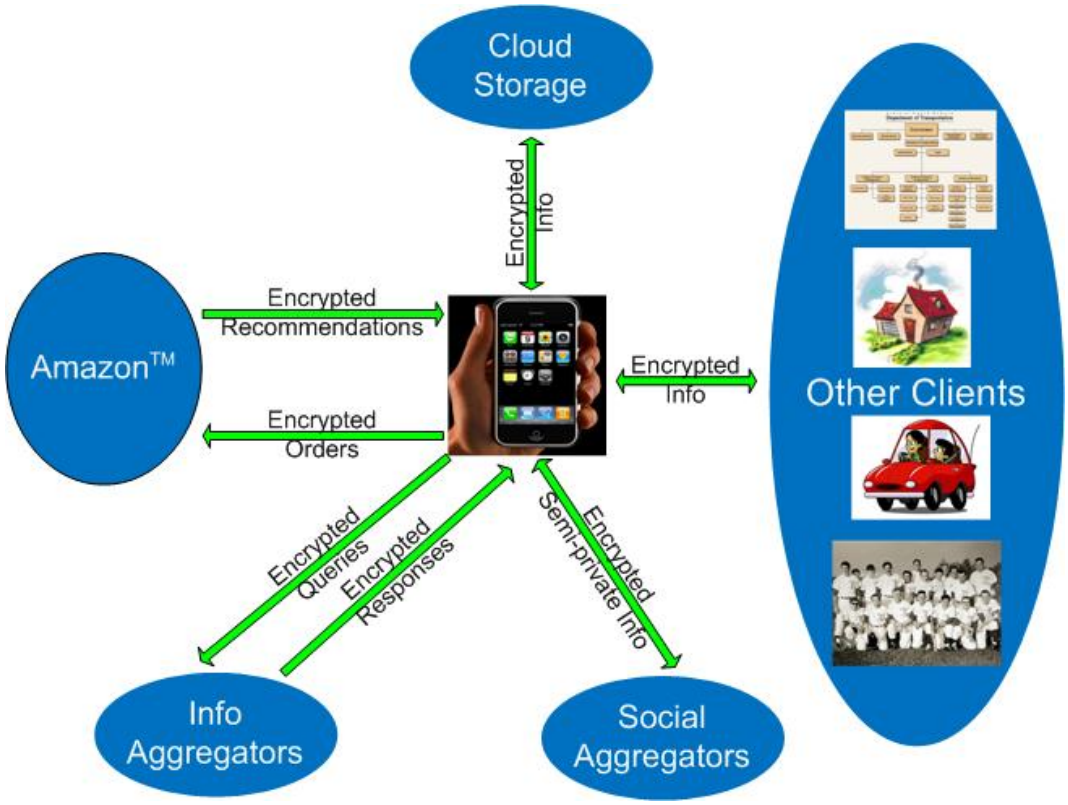
> *We are very early in the total information we have within Google." ...The goal is to enable Google users to be able to ask the question such as ˜What shall I do tomorrow? and ˜What job shall I take?...****We cannot even answer the most basic questions because we don't know enough about you. That is the most important aspect of Google's expansion.***

***The more a smartphone knows about its user, the more it can do in the way of helpful information services.*** Ultimately, there will be very few secrets between a user and their smartphone. ***And the more a smartphone knows about its user, the better job it can do targeting ads***. Merchants are willing to pay a lot for well-targeted ads that result in increased business.

## Performing information integration using customer equipment

**Many customers value their proprietary information and privacy. They do not want to have their intimate private information stored unencrypted in aggregator datacenters where it can be subpoenaed and observed by an aggregator's employees**. According to Mark Zuckerberg's 2004 Email Break-In Could Be A Felony

> *Mark Zuckerberg's hacking of email accounts and user profiles in 2004 could be felonies under Federal and state law, according to privacy lawyers...*
>
> ***Mark now oversees private data of 400 million people as the CEO of Facebook. Questions have been raised about whether this 2004 behavior violated laws and whether users can trust the company to keep their information from being misused****.* (emphasis added)




# Protecting Intimate and Proprietary Information

Datacenter integration will face the challenge of emerging competitors that will perform information integration using customer equipment instead of cloud datacenters. As explained below, these competitors will have important advantages over datacenter integration including increased revenue from better targeted advertising, lower operational costs, fewer requirements for government regulation, and greater customer and advertiser satisfaction.

### Lower Costs

Information integration can be computationally intensive. It's less expensive for competitors to perform integration using customer equipment than datacenter integration. Also, competitors using client information integration will have lower communications costs than datacenter integration because communication by clients with datacenters will be less necessary.

### Faster Response

Because it is less necessary to communicate with datacenters, competitors using client information integration can provide faster response than datacenter integration because most needed information will already be cached in the customer equipment.

### Less Regulation

By performing information integration in customer equipment, competitors can store customer information in datacenters encrypted so that it can be decrypted only using the customer's private key. In this way, there will be less requirement for regulating these competitors than those using datacenter integration because they will have less intimate private information in their datacenters.

Of course, competitors that perform information integration on customer equipment will provide convenient ways for customers to share their information. For example, personal medical information will be sent out that can be decrypted by their medical providers. Also, appropriate information feeds will be provided for social sharing with family, friends, colleagues, and followers.

In summary, competitors can make more money with greater customer and advertiser satisfaction by integrating information using customer equipment than datacenter integration. Also, there will fewer requirements for the government to regulate them.

# Private Information Challenges

According to Facebook's Zuckerberg Says the Age of Privacy Is Over,

> Mark Zuckerberg (founder and CEO of Facebook) at TechCrunch 2010 said *A lot of companies would be trapped by the conventions and their legacies of what they've built* [less than two years ago Zuckerberg said privacy control is *the vector around which Facebook operates*], *doing a privacy change* - ***doing a privacy change for 350 million users is not the kind of thing that a lot of companies would do....we decided that these would be the social norms now and we just went for it.*** •
>
> ***Now that it has 350 million people signed up and connected to their friends and family in a way they never have been before - now Facebook decides that the initial, privacy-centric, contract with users is out of date. That users actually want to share openly, with the world at large, and incidentally (as Facebook's Director of Public Policy Barry Schmitt told me in December) that it's time for increased pageviews and advertising revenue, too.*** (emphases added)

According to Facebook Glitch Brings New Privacy Worries,

> **[Facebook]** ***users discovered a glitch that gave them access to supposedly private information in the accounts of their Facebook friends, like chat conversations***.
>
> *Not long before,* ***Facebook had introduced changes that essentially forced users to choose between making information about their interests available to anyone or removing it altogether***.
> (emphases added)

According to a brief by the Electronic Frontier Foundation:

> *Power Ventures sought to provide Facebook users with a tool that could, at the users' direction, aggregate their Facebook inbox messages, friend lists and other data with messages and lists from other social networks the individual patronizes, such as Orkut or LinkedIn. Power's product allowed Facebook users to view all of their different social network data in one place.* ***Facebook users benefited from the choice Power offered them in how to access and use their social network data across several different social networks.***
>
> ***Facebook argues that by offering these enhanced services to users, Power violated California's computer crime law. Power's efforts to ensure that Facebook's authorized users could continue to access their own data on Facebook's servers despite Facebook's attempts to control the means of access should not trigger criminal liability. Imposing such sanctions here will also hobble user choice and interfere with follow-on innovation, in part by creating a barrier to Facebook users who wish to move their data from Facebook to a competing service. Perhaps the most important fact in this case is that Power's servers only connect with Facebook servers at the behest of a Facebook user, who must provide her own valid username and password to obtain access to Facebook and her own social networking data. Power did not connect to Facebook except as an agent of an authorized user. Importantly, Facebook users own the information they store with the company. The Facebook terms of service confirm this and it is not subject to dispute.***
>
> *As part of its business model, Facebook has also steadily increased the amount of information about its users and their activities it offers to third parties. Facebook has an Application Programming Interface, or API, through which third parties can see the information and activities of Facebook's users.* ***Through controversial changes to its terms of service and the functionality of its API, Facebook now offers to certain third parties and advertisers as much information about any particular user and his or her friends as that user personally could have accessed using Power's service****. Thus, by continuing to press for Power to be liable under criminal law,* ***Facebook's actions appear to be aimed not at protecting users from the sharing of their information with third parties, but at ensuring Facebook's own control (and the corresponding ability to monetize) user information, even against the users themselves.*** (Emphases added.)

In 8 Million Reasons for Real Surveillance Oversight (emphasis added)

> ***Sprint Nextel provided law enforcement agencies with its customers' (GPS) location information over 8 million times between September 2008 and October 2009.*** *This massive disclosure of sensitive customer information was made possible due to the roll-out by Sprint of a new, special web portal for law enforcement officers.*

In Justice Department wants cell phone locations without warrant, (emphasis added)

***Should the government be able to track your movements based on cell-phone records, without evidence of criminal wrongdoing?***

*A legal showdown on the closely watched issue unfolded Friday in a federal appeals court in Philadelphia, as the Justice Department battled electronic-privacy groups.*

***. The Justice Department wants to get the cell-phone location information without showing probable cause of a crime. Opponents say the data could show when someone visits a church, medical clinic or political rally.***

***Appellate Judge Dolores Sloviter wondered aloud what a rogue government might do with such information.***

In Comments of the World Privacy Forum to FTC on Nov. 6, 2009 (emphases added)

***Note for example the MedNet Mental Health Problems list. We think that many of the consumers named on this list are not likely to know they are on the list. We also think that many of the consumers named on this list would like the option to delete their names and identifying information from this list.***

***In this list, 2,985,634 consumers with wide-ranging mental health issues are identified, including segmented categories of people with depression, poor memory, autism, eating disorders, and other states this list identifies as mental problems. The data card for this list states:***

> ***Mental health problems can create a significant burden on the afflicted individual, making them extremely receptive to any campaign that may be able to offer some assistance or relief. •***

*Returning to the issue of targeted marketing and how consumers purportedly like it**, it is unlikely that the caretaker of an autistic adult would be happy to know that this person is being targeted because he or she will be extremely receptive to certain types of campaigns.***

***We also think that some of the 6 million people on the Credit Card Declines marketing list would like to know they are on a list of people who have been declined for major bank cards, and would like the opportunity to delete their age, the age of their children, the gender of their child, dwelling type, ethnicity, and other information from the list and databases associated with it.***

According to Buzz has privacy issues and it's Google's default, (emphasis added)

***You can understand Google wanting to get a piece of all that social networking and status updating traffic, and you can understand why it would prefer those who use the new Buzz social features in Gmail to do so as widely and openly as possible. But looking at the assumptions behind the default Buzz setup, you have to wonder whether the Googlers have so thoroughly embraced the vision of one great world of sharing that they've grown out of touch with the privacy concerns of the rest of us.***

*If that's the case, then there's probably some dismayed surprise around the Googleplex today at the backlash over the implementation of Buzz. Among the complaints:*

- *Buzz automatically sets you up with followers and other users to follow, based on the Gmail contacts you most often e-mail or chat with. This is awkward enough, since those contacts may include business associates or others who don't qualify as share-worthy friends. But more troublesome, unless you edit your settings, the list of followers and followees can be seen by anyone on your Google profile page" a very public showcase of the people you're in touch with most often.*
- *If you use the vanity URL on your Google Profile page, that identifies your Gmail address, and if anyone sends an @ reply to you via Buzz, they are broadcasting that address far and wide.*
- *On the mobile side of Buzz, if you choose to Share Location, you should know that you're sharing not only with your followers but with anybody who happens to be scanning the Buzz entries in a particular geographic area.*

According to Critics Say Google Invades Privacy With New Service, (emphasis added)

*Many users bristled at what they considered an invasion of privacy, and they faulted the company for failing to ask permission before sharing a person's Buzz contacts with a broad audience. For the last three days, Google has faced a firestorm of criticism on blogs and Web sites, and it has already been forced to alter some features of the service.*

*E-mail, it turns out, can hold many secrets, from the names of personal physicians and illicit lovers to the identities of whistle-blowers and antigovernment activists. And Google, so recently a hero to many people for threatening to leave China after hacking attempts against the Gmail accounts of human rights activists, now finds itself being pilloried as a clumsy violator of privacy.*

***As Evgeny Morozov wrote in a blog post for Foreign Policy, If I were working for the Iranian or***

***the Chinese government, I would immediately dispatch my Internet geek squads to check on Google Buzz accounts for political activists and see if they have any connections that were previously unknown to the government."***

According to Google Buzz privacy flaw snags another victim: White House Deputy CTO Andrew McLaughlin

*Well, now we've learned that one of those who apparently got swept up in the Buzz privacy imbroglio was none other than Andrew McLaughlin, the controversial Deputy Chief Technology Officer in the Obama White House* ***who was formerly Google's top lobbyist.***

*McLaughlin works in the White House Office of Science and Technology Policy (OSTP) and is in charge of all Internet policy for the Administration. The two key components of OSTP's mission are the creation of an Open and Transparent Democracy, and ironically, Safeguarding the Privacy of Every American by* ***holding businesses accountable for violations of personal privacy.***

*McLaughlin's Buzz profile (which he quickly made private after his contacts were exposed) is enlightening to say the least. It includes a treasure trove of movers and shakers in high-tech, Internet public policy, and venture capital circles.*

*But it includes much, much more. At least 28 of the folks Google Buzz pulled from McLaughlin's Gmail contact list are employed by Google including a who's who of Google senior lobbyists and lawyers from across the globe.* (emphases added)

According to Dave Winer in Google did something seriously wrong,

*Here's what happened. When Google rolled out Buzz last week they activated an unknown number of users and chose people for them to follow automatically based on who they email most frequently with. Presumably these people had to also be on Gmail. And the list of people you follow is public. Therefore the list of people you email with most frequently is now public. They are now trying to close this hole as quickly as possible. But the damage is done, people have to realize that -- the information was already disclosed. You can close the door after the horse gets out but that doesn't get the horse back.*

***This never should have happened. But now that it has, it requires a CEO-level apology and statement of contrition and an explanation of what policies he's putting in place to be sure this never happens again.***

According to Google Data Admission Angers Europe,

*in Germany,* ***Google's collection of the data --- which the company said could include the Web sites viewed by individuals or the content of their e-mails â€" is a violation of privacy law****, said Ilse Aigner, the German federal minister for food, agriculture and consumer protection.*

*Based on the information we have before us, it appears that Google has illegally tapped into private networks in violation of German law, Ms. Aigner said. This is alarming and further evidence that privacy law is a foreign concept to Google."*

*Johannes Caspar, the data protection supervisor who is leading the German government's dealings with Google on the issue, said the company's revelation of illegal data collection will be taken up by the Article 29 Working Party, a panel of European national data protection chiefs that advises the European Commission.*

*"I am glad that this cat-and-mouse game with Google is finally over, Mr. Caspar said.*

*Initially, Google had told German officials that the data it had collected was limited to just two bits of information: the publicly broadcast ID number of the device, which is called a MAC address, and the name assigned to it by the owner.* (emphases added)

According to Germany Questions Google's Data Mistake •

*So everything was a simple oversight, a software error!* [Peter] *Schaar* [Germany's federal commissioner for data protection and freedom of information] *wrote. The data was collected and stored against the will of the project's managers and other managers at Google. If we follow this logic further, this means:* ***The software was installed and used without being properly tested beforehand. Billions of bits of data were mistakenly collected, without anyone in Google noticing it, including Google's own internal data protection managers, who two weeks ago were defending to us the company's internal data protection practices.***

***Have to admit, he does have a point. How does a company with Google's smarts and technological acumen collect and store Wi-Fi network payload data in more than 30 countries for three years without being aware of it?***

*Mistakes are made, I suppose. But the breadth of this one is pretty incredible. As Marc Rotenberg, executive director of the Electronic Privacy Information Center, told the Financial Times,* ***This may be one of the most massive surveillance incidents by a private corporation that has ever occurred. It is unprecedented vacuuming of WiFi data by a private company. Can you imagine what would happen if a German corporation was sending cars through Washington sucking up all this information?*** (emphases added)

According to an interview with Marissa Mayer, Vice-president of Search Products and User Experience at Google (Marissa Mayer: An omnivorous Google is coming):

***She [Mayer] wants Google to be capable of presenting information to users before they even know what they're looking for.*** *Amazingly she doesn't think her team [is] that far away from achieving what she calls the omnivorous search engine - i.e.,* ***one which is able to take a user's total context - where they are, what they were just reading, which direction their mobile phone is pointed and so on.*** (emphasis added)

According to Vermont Court Rules in Encryption Self-Incrimination Case,

*In a long-awaited decision in the case of Sebastian Boucher, In re Grand Jury Subpoena to Sebastian Boucher, 2009 U.S. Dist. LEXIS 13006, No. 2:06-mj-91 (D. Vermont Feb. 19, 2009), the court held that Mr. Boucher did not enjoy a Fifth Amendment right to refuse to provide the Government with an un-encrypted version of files seized by law enforcement agents and suspected of containing child pornography.*

*The case is interesting at many levels. Child porn is a scourge. Equally pernicious, however, is the view that* ***there is nothing an individual can do to keep the prying eyes of the government and others away from intensely personal information.*** *This case will almost certainly be appealed. So, stay tuned.* (emphasis added)

In Leading Privacy Organization Warns that Privacy Problems Cannot Be Fixed,

*At a hearing in New York federal district court, Electronic Privacy Information Center (EPIC), President Marc Rotenberg urged Judge Denny Chin to reject the proposed Google Books settlement. Mr. Rotenberg described how the proposed deal fails to protect readers' privacy while mandating collection of readers' sensitive, personal information. A person at any library or any university in the United States that attempted to retrieve information from Google's digital library would be uniquely tagged and tracked, Mr. Rotenberg warned. There is simply no precedent for the creation of such power.* (emphasis added)

According to Breaking a Promise on Surveillance

*It is just a technical matter, the Obama administration says:* ***We just need to make a slight change in a law to make clear that we have the right to see the names of anyone's e-mail correspondents and their Web browsing history without the messy complication of asking a judge for permission****...*

***These national security letters are the same vehicles that the Bush administration used after the Sept. 11, 2001, attacks to demand that libraries turn over the names of books that people had checked out. The F.B.I. used these letters hundreds of thousands of times to demand records of phone calls and other communications, and the Pentagon used them to get records from banks and consumer credit agencies. Internal investigations of both agencies found widespread misuse of the power, and little oversight into how it was wielded***.(emphases added)

# Foreign Security Services Blackmail Threat

The US government has the power to compel a company over which it has jurisdiction to secretly turn over information on foreign nationals and foreign companies in the company's data centers.

According to Iceland summons US envoy over demand for MP's Twitter details

*The American ambassador to Iceland has been summoned to explain why US officials are trying to access the Twitter account of an Icelandic MP and former WikiLeaks collaborator.*

*Birgitta Jónsdóttir, an MP for the Movement in Iceland, revealed last week that the US justice department had asked Twitter to hand over her information. The US authorities are trying to build a criminal case against the website after its huge leaks of classified US information.*

*"[It is] very serious that a foreign state, the United States, demands such personal information of an*

*Icelandic person, an elected official," the interior minister, Ogmundur Jonasson, told Icelandic broadcaster RUV. "This is even more serious when put [in] perspective and concerns freedom of speech and people's freedom in general," he added.*

The Australian Environment and Communications References Committee Report of April 2011 said:

*The committee further recommends that all Australian organizations* [including foreign companies that operate in Australia] *which transfer personal information overseas, including small businesses, must ensure that the information will be protected in a manner at least equivalent to the protections provided under Australia's privacy framework.*

Countries outside the US are considering imposing restrictions on companies operating within their borders with regard to US government access to information on their people and companies stored in the companies' data centers.

# Regulating Aggregator Datacenters

However, serious discussions have begun on the implications of having intimate personal information stored in datacenters (see Is intimate personal information a toxic asset in client-cloud datacenters?). On December 7, 2009, the Federal Trade Commission held a workshop on *Exploring Privacy* including the benefits and risks of collecting, using, and retaining customer data. These discussions will inevitably result in strong government regulation. Aggregator employees will be personally required to respect confidentiality of intimate personal information. Also, aggregators will be restricted how they can share information with third parties. Paradoxically, strong government regulation can be helpful to datacenter integration by legitimatizing their business model: Instead of having to say *Trust us* aggregators will be able to say **By law we must preserve confidentiality of information in our datacenters.** Developing these regulations will require a synthesis of best practices from those that currently govern handling intimate personal information by legal and health practitioners.

Client information integration can be more helpful to a customer because there will be some of the customer's information that is not available in an aggregator's datacenters since it is stored elsewhere, e.g., Amazon, other aggregators, etc. Customer equipment can integrate information from *all* relevant sources together with immediate personal physical, psychological, physiological, medical, and social information that is not available in an aggregator's datacenters. Because customer equipment has access to *all* the user's information, competitors will have an advantage that they can make advertising much more relevant and useful.

Awareness is growing concerning the competitive disadvantage in doing information integration in datacenters: an aggregator will not have all of a customer's information in its datacenters. In The next step in cloud computing is to link different systems, Vint Cerf proposed:

*I think we need to start developing interfaces so that clouds can communicate directly among themselves...Interactions among clouds would appear to be happening through an intermediate virtual cloud. In this model, each cloud could translate its internal method of organizing data to and from standardized naming conventions, data exchange protocols, and perhaps data description protocols.*

Given the sensitivity of the intimate personal information involved, these arrangements between aggregators will also need to be regulated. Clients will be able to use virtual cloud interfaces to interact with each other and with cloud datacenters.

Furthermore, virtual cloud interfaces will make it feasible for government security and justice agencies to integrate information from datacenters of multiple aggregators. Consequently there may be external security dangers as well. For example in Google attack part of widespread spying effort

*That's because they* [the attacks from China] *apparently were able to access a system used to help Google comply with search warrants* [and National Security Letters see below] *by providing data on Google users, said a source familiar with the situation, who spoke on condition of anonymity because he was not authorized to speak*

*with the press. "Right before Christmas, it was, 'Holy s***, this malware is accessing the internal intercept [systems],'" he said.*

According to National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments by the Congressional Research Service:

> A National Security Letter is a form of administrative subpoena used by the United States Federal Bureau of Investigation and reportedly by other U.S. Government Agencies including the Central Intelligence Agency and the Department of Defense. It is a demand letter issued to a particular entity or organization to turn over various record and data pertaining to individuals. They require no probable cause or judicial oversight. They also contain a gag order, preventing the recipient of the letter from disclosing that the letter was ever issued.
>
> *From 2003 through 2005, the FBI issued at least 143,074 National Security Requests.*

Aggregator internal security problems are an additional threat:

> *Google is investigating whether one or more employees may have helped facilitate a cyber-attack that the U.S. search giant said it was a victim of in mid-December* [see above], *two sources told Reuters on Monday.* (in Google probing possible inside help on attack)

According to Google Asks Spy Agency for Help With Inquiry Into Cyberattacks

> *By turning to the N.S.A., which has no formal legal authority to investigate domestic criminal acts, instead of the Department of Homeland Security, which does have such authority, Google is clearly seeking to avoid having its search engine, e-mail and other Web services regulated as part of the nation's critical infrastructure.*
>
> *Google and N.S.A. are entering into a secret agreement that could impact the privacy of millions of users of Google's products and services around the world, said Marc Rotenberg, executive director of the Electronic Privacy Information Center, a Washington-based policy group. On Thursday, the organization filed a lawsuit against the N.S.A. calling for the release of information about the agency's role as it was set out in National Security Presidential Directive 54, a classified 2008 order issued by former President Bush dealing with cybersecurity and surveillance.*

According to Feds thinking outside the box to plug intelligence gaps

> **Still another program, called Knowledge Discovery and Dissemination [KDD], might have helped detect Umar Farouk Abdulmutallab, the Nigerian bombing suspect who's alleged to have nearly caused a tragedy on Christmas Day in spite of a raft of clues, which weren't put together in time**.
>
> ***IARPA [Intelligence Advanced Research Projects Activity] claims that KDD projects could improve massive databases that don't mesh well with one another, allowing key connections to go undetected***.
>
> *In the Christmas bombing case, "the dots simply were not connected," Russell Travers, a deputy director at the National Counterterrorism Center, told the Senate Judiciary Committee last week at a hearing on the incident. "**The U.S. government needs to improve its overall ability to piece together partial, fragmentary information from multiple collectors**."* (emphases added)

According to the Electronic Frontier Foundation in NSA Spying:

> ***The U.S. government, with assistance from major telecommunications carriers including AT&T, has engaged in a massive program of illegal dragnet surveillance of domestic communications and communications records of millions of ordinary Americans since at least 2001.***
>
> *News reports in December 2005 first revealed that the National Security Agency (NSA) has been intercepting Americans' phone calls and Internet communications. Those news reports, plus a USA Today story in May 2006 and the statements of several members of Congress, revealed that the NSA is also receiving wholesale copies of their telephone and other communications records. All of these surveillance activities are in violation of the privacy safeguards established by Congress and the U.S. Constitution.*

According to Police want backdoor to Web users' private data (emphases added)

> *Anyone with an e-mail account likely knows that police can peek inside it if they have a paper search warrant.*
>
> ***But cybercrime investigators are frustrated by the speed of traditional methods of faxing, mailing, or e-mailing companies these documents. They're pushing for the creation of a national Web interface linking police computers with those of Internet and e-mail providers so requests can be sent and received electronically***.
>
> *CNET has reviewed a survey scheduled to be released at a federal task force meeting on Thursday, which says*

*that law enforcement agencies are virtually unanimous in calling for such an interface to be created. Eighty-nine percent of police surveyed, it says, want to be able to exchange legal process requests and responses to legal process through an encrypted, police-only nationwide computer network. (See one excerpt and another.)*

*The survey, according to two people with knowledge of the situation, is part of* ***a broader push from law enforcement agencies to alter the ground rules of online investigations. Other components include renewed calls for laws requiring Internet companies to store data about their users for up to five*** *years ....*

***But the most controversial element is probably the private Web interface, which raises novel security and privacy concerns, especially in the wake of a recent inspector general's report (PDF) from the Justice Department. The 289-page report detailed how the FBI obtained Americans' telephone records by citing nonexistent emergencies and simply asking for the data or writing phone numbers on a sticky note rather than following procedures required by law****.*

*Some companies already have police-only Web interfaces. Sprint Nextel operates what it calls the L-Site, also known as the legal compliance secure Web portal. The company even has offered a course that will teach you how to create and track legal demands through L-site. Learn to navigate and securely download requested records.*

*The police survey is not exactly unbiased: its author is Frank Kardasz, who is scheduled to present it at a meeting (PDF) of the Online Safety and Technology Working Group, organized by the U.S. Department of Commerce. Kardasz, a sergeant in the Phoenix police department and a project director of Arizona's Internet Crimes Against Children task force, said in an e-mail exchange on Tuesday that he is still revising the document and was unable to discuss it.|*

***In an incendiary October 2009 essay, however, Kardasz wrote that Internet service providers that do not keep records long enough are the unwitting facilitators of Internet crimes against children" and called for new laws to "mandate data preservation and reporting. He predicts that those companies will begin to face civil lawsuits because of their lethargic investigative process.***

According to Technology Coalition Seeks Stronger Privacy Laws

*A broad coalition of technology companies including AT&T, Google and Microsoft, and advocacy groups from across the political spectrum said Tuesday that it would push Congress to strengthen online privacy laws to protect private digital information from government access.*

*Under a proposed set of principles,* ***law-enforcement agencies or other government representatives would have to obtain a search warrant based on a showing of probable cause before they could access a person's e-mail, photos or other electronic documents stored in a cloud based service like Gmail, Flickr or Facebook. Under current law, much of that information is accessible through a simple subpoena*** **[e.g. a National Security Letter],** ***which can be issued under looser rules.***

*Obtaining access to information about where people are located or the places they visited would be protected under the same standard. Currently, courts are divided on whether access to location information requires a warrant or a subpoena. Members of the coalition acknowledged they would probably face resistance from law-enforcement agencies.* ***This year, Justice Department lawyers argued in court that cellphone users have given up the expectation of privacy about information about their location by voluntarily giving that information to cellphone companies.***(emphases added)

# "Nothing to hide" argument

According to Eric Schmidt (CEO Google):

***If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place****. If you really need that kind of privacy, the reality is that* ***search engines -- including Google -- do retain this information*** *for some time and it's important, for example, that we are all subject in the United States to the Patriot Act and* ***it is possible that all that information could be made available to the authorities****.* (emphases added)

According to Bruce Schneider in My Reaction to Eric Schmidt

***Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance.***

*We do nothing wrong when we make love or go to the bathroom. We are not deliberately hiding anything when we seek out private places for reflection or conversation. We keep private journals, sing in the privacy of the shower, and write letters to secret lovers and then burn them. Privacy is a basic human need.*

***For if we are observed in all matters, we are constantly under threat of correction, judgment, criticism, even plagiarism of our own uniqueness. We become children, fettered under watchful eyes, constantly fearful that -- either now or in the uncertain future -- patterns we leave behind will be brought back to implicate us, by whatever authority has now become focused upon our once-private and innocent acts****. We lose our individuality*

[and dignity], *because everything we do is observable and recordable.*

*This is the loss of freedom we face when our privacy is taken from us. This is life in former East Germany, or life in Saddam Hussein's Iraq. And it's our future as we allow an ever-intrusive eye into our personal, private lives.*

***Too many wrongly characterize the debate as "security versus privacy." ...Liberty requires security without intrusion, security plus privacy. Widespread police surveillance is the very definition of a police state. And that's why we should champion privacy even when we have nothing to hide***. (emphases added)

# Taxonomy of Private Information Violations

Daniel Solove developed the following taxonomy of privacy violations in 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy:

***Information Collection*****:** *Surveillance, Interrogation*
***Information Processing*****:** *Aggregation, Identification, Insecurity, Secondary Use, Exclusion*
***Information Dissemination*****:** *Breach of Confidentiality, Disclosure, Exposure*
***Increased Accessibility*****:** *Blackmail, Appropriation, Distortion, Invasion, Intrusion****,*** *Decisional Interference*

*The taxonomy has four general categories of privacy problems with sixteen different subcategories. The first general category is information collection, which involves the ways that data is gathered about people. The subcategories, surveillance and interrogation, represent the two primary problematic ways of gathering information.* ***A privacy problem occurs when an activity by a person, business, or government entity creates harm by disrupting valuable activities of others. These harms need not be physical or emotional; they can occur by chilling socially beneficial behavior (for example, free speech and association) or by leading to power imbalances that adversely affect social structure (for example, excessive executive power)***.(emphases added)

# Draft Internet Bill of Rights

Of course, in considering possible regulation, there are important pitfalls to be avoided including the following that have previously occurred: inhibited innovation, stifled startups, annoyed and confused consumers, failed to address consumer and enterprise concerns making them reluctant to use valuable client-cloud services, imposed inefficient (and sometimes harmful) methods, processes and procedures, and prevented adoption of best practices

Below is a draft bill of rights that attempts to avoid the above pitfalls:

- **Information Disclosure.** *Clients have the right to receive accurate, timely, easily understood information in making informed decisions about their personal information (including that which could be used to help identify, contact or locate them) held by Internet information aggregators.*
- **Confidentiality of Information.** *Clients have the right to communicate with their aggregators in confidence and to have the confidentiality of their personal information protected. Clients also have the right to review and copy their own information and request amendments and deletions.*
- **Security of Information.** *Clients have the right to security of their information and to timely disclosure of security breaches. For example, they have the right to the means to reliably remove rootkits, viruses, spyware, and other malware from their own equipment.*
- **Participation in Advertising Decisions.** *Clients have the right to participate in the process of being offered advertisements based on their information. Clients who are unable to fully participate in the process of being offered advertisements have the right to be represented by parents, guardians, family members, or other conservators.*
- **Respect and Nondiscrimination**. *Clients have the right to considerate, respectful treatment from Internet information aggregators at all times and under all circumstances.*
- **Complaints and Appeals.** *Clients have the right to a fair and efficient process for resolving differences with their aggregators, and the institutions that serve them, including a rigorous system of internal review and an independent system of external review*

According to a Zogby International poll of a representative sample population of the US:

- *Eight in ten (80%) are concerned with companies recording their online habits and using the data to generate profit through advertising, and a fifth (19%) are not.*
- *Nine in ten (88%) believe that tracking where Internet users go on the Internet without their permission is an unfair business practice, while 7% believe it is a fair practice.*

- *Half (49%) believe government regulators should play a larger role in protecting online consumer privacy, and more than a third (36%) do not.*
- *The large majority (88%) believe consumers should enjoy similar legal privacy protections online as they have offline, while 4% do not.*
- *Eight in ten (79%) support a national Do Not Track List, similar to the current national Do Not Call List, to prevent tracking where people go on the Internet, and 6% do not.*

# Separation of Content, Transport, and User Operations

Separation of powers is a fundamental principle of government that is enshrined in the US Constitution. To prevent conflicts of interest, each Internet vendor should be restricted to competing in just one of the following:

1. ***Content**, e.g.*, Columbia Pictures, Disney, Huffington Post, NY Times
2. ***Transport**, e.g.*, cable, wireless, satellite
3. ***User Operations**, e.g.*, operating systems like Windows, iOS, Android

According to Tim Wu in *The Master Switch* [Knoph 2011]:

> *A Separations Principle would make the creation of a salutary distance between each of the major functions or layers in the information economy. It would mean that that those who develop information, those who own the network infrastructure on which it travels, and those who control the tools or venues of access must be kept apart from each other...**A strong stake in more than one layer of the industry leaves a firm in a position of inherent conflict of interest...the objectives of creating information are often at odds with those of disseminating it.***
>
> *Under such a rule, a merger of Comcast, the emerging broadband monopolist for much of the nation, with NBC or Disney---a combination obviously resulting in the sort of conflicts of interest a Separations Principle is meant to prevent---would simply be out of the question; it would thus not be subject to the **customary gaming of the commission's approval process whereby applicants offer marginal concessions in exchange for extravagant license.***

On January 18, 2011, the FCC approved the acquisition of NBC by Comcast representing the first time that a cable company will control a major broadcast network. According to the Brian Stelter and Tim Arango in the NY Times (emphasis added):

> *The F.C.C. vote was 4 to 1, with the senior Democratic commissioner, Michael J. Copps, casting the dissenting vote. Mr. Copps, who had expressed doubt in the past about whether the combination would benefit consumers, said in a statement Tuesday that **it confers too much power in one company's hands**. •*
>
> *Mr. Copps also said, **The Comcast-NBCU joint venture opens the door to the cable-ization of the open Internet. The potential for walled gardens, toll booths, content prioritization, access fees to reach end users, and a stake in the heart of independent content production is now very real**. •*

In his statement, Copps said (emphasis added):

> *at the end of the day **this transaction is a huge boost for media industry (and digital industry) consolidation**. It puts new media on a road traditional media should never have taken. **It further erodes diversity, localism and competition "the three essential pillars of the public interest standard mandated by law.** I would be true to neither the statute nor to everything I have fought for here at the Commission over the past decade if I did not dissent from what I consider to be a damaging and potentially dangerous deal.*

# Acknowledgments

Ross Anderson, Ryan Calo, David Dill, Dan Flickinger, Blaine Garst, Michael Genesereth, Alyssa Glass, Axel Hochstein, Chuck House, Mike Huhns, Anita Jones, Eric Kao, Michael Kassoff, Gerard Kiley, Tolga Konik, Monica Lam, Martha Russell, Tim O'Reilly, Charles Petrie and Bill Wulf made comments and suggestions that greatly improved this article. Of course, none of these colleagues are responsible for my entirely personal views expressed in this article.