The Pirated “I”
or How Privacy Can’t Exist on a Lawless Semantic Web

Abe Hsuan
June 2, 2011
Sony PlayStation suffers massive data breach

Tue, Apr 20 2011

By Liana B. Baker and Jim Finkle

NEW YORK/BOSTON (Reuters) - Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts in what is one of the largest-ever Internet security break-ins.

Sony learned that user information had been stolen from its PlayStation Network seven days ago, prompting it to shut down the network immediately. But Sony did not tell the public until Tuesday.

The electronics conglomerate is the latest Japanese company to come under fire for not disclosing bad news quickly. Tokyo Electric Power Co was criticized for how it handled the nuclear crisis after the March earthquake. Last year, Toyota Motor Corp was slammed for being less than forthright about problems surrounding its massive vehicle recall.
Congress Deepens Apple Probe Over Location Tracking

First Posted: 04/28/11 06:21 PM ET ; Updated: 04/28/11 06:21 PM ET

React > Inspiring | Funny | Obsolete | Scary | Must-Have | Amazing | Innovative | Nerdy

Follow > Al Franken, Apple Iphone, Iphone, Iphone 4, House Energy And Commerce Committee, Ios, Privacy, Security, Technology News
Google, Apple To Testify At Congressional Hearing Over Location Tracking And Privacy

First Posted: 06/06/11 09:16 AM ET; Updated: 06/06/11 09:16 AM ET

React: Inspiring money, Obsolete, Scary, Must-Have, Amazing, Innovative, Nerdy

WASHINGTON (Reuters) - Tech companies such as Apple and Google are hoping the tracks of millions of mobile device users will lead to billions of dollars in revenue.
Google Street View broke Canada's privacy law with Wi-Fi capture
Commissioner says Google committed 'serious violation' of privacy laws

Josh Halliday
guardian.co.uk, Wednesday 20 October 2010 07.30 BST
Google Street View broke Canada's privacy law with Wi-Fi capture

Get Ready For A Flurry Of New Online-Privacy Bills In Congress

Legislators in the House and the Senate are now practically falling over each other to introduce new online-privacy legislation. Congressional aides told Capitol Hill newsletter The Hill that Rep. Jackie Speier (D-Calif.) and Rep. Bobby Rush (D-Ill.) will both introduce privacy bills next week, and at least one Republican will also be introducing a bill.

WASHINGTON (Reuters) - Tech companies such as Apple and Google are hoping the tracks of millions of mobile device users will lead to billions of dollars in revenue.
Massive Epsilon email breach hits Citi, Chase, more

Numerous companies' databases have been compromised due to unauthorized entry into Epsilon's email system

By Sarah Jacobsson Purewal | PC World

The Epsilon e-mail breach has escalated into a “massive breach,” according to SecurityWeek blogger Mike Lennon.

The breach was first noted on March 31, when Epsilon, a marketing firm whose services include permission-based email marketing and database hosting, began notifying its customers of potential data exposure thanks to an unauthorized entry into Epsilon's email system. According to Epsilon, the information compromised was “limited to email addresses and/or customer names only,” and “no other personal identifiable information

The Epsilon e-mail breach has escalated into a “massive breach,” according to SecurityWeek blogger Mike Lennon.

The breach was first noted on March 31, when Epsilon, a marketing firm whose services include permission-based email marketing and database hosting, began notifying its customers of potential data exposure thanks to an unauthorized entry into Epsilon's email system. According to Epsilon, the information compromised was “limited to email addresses and/or customer names only,” and “no other personal identifiable information
News Corp.'s Myspace Sued for Giving Away Data on Members Without Consent

By Thom Weidlich - Apr 13, 2011 8:02 PM ET

News Corp. (NWSA)'s Myspace unit was accused in a lawsuit of giving data to aggregators that are used to associate members by name with their Internet browsing history without their consent.

Myspace shares the data with aggregators despite telling members they can restrict access to their information, according to the complaint filed today in federal court in Brooklyn, New York. The suit, filed by New York law firms Milberg LLP and Reese Richman LLP, seeks class-action, or group, status and unspecified damages.

"Myspace knowingly serves as and profits handsomely from being a conduit through which details of the most intimate aspects of its members' lives, as reflected in their Internet browsing history and otherwise, are transmitted to data aggregators, who package the information into profiles and sell it like any other commodity to advertisers," according to the complaint.
Kerry: 'Do-Not-Track' Tool Insufficient To Protect Privacy

The Kerry-McCain privacy bill, introduced in the Senate yesterday, would for the first time give consumers the right to opt out of behavioral targeting. While industry self-regulatory groups have long said that ad networks should let people opt out of ad targeting anyway, those standards are voluntary. The Commercial Privacy Bill of Rights, by contrast, would be mandatory.

Yet it seems like the bill isn’t drawing nearly as much attention for what it includes as for what it leaves out: The proposal doesn’t specifically refer to a do-not-track mechanism that would allow users to opt out of all online tracking at once.
Kerry: 'Do-Not-Track' Is Insufficient To Protect Privacy

The Kerry-McCain privacy bill, introduced yesterday, would for the first time give consumers the right to opt out of behavioral targeting. While some regulatory groups have long said that it's not enough to let people opt out of ad targeting and that these measures are voluntary. The Commercial Privacy Bill of Rights, in contrast, would be mandatory.

Yet it seems like the bill isn't drawing much attention for what it includes as for what it excludes. The proposal doesn't specifically refer to a "Do-Not-Track" mechanism that would allow users to opt out of being tracked at once.

John Paczkowski

EU Slams Google, Microsoft and Yahoo Over Data Retention

MAY 27, 2010 AT 9:28 AM PT

The privacy practices of the world's three largest search engines are under fire in Europe again. European Union officials sent letters to Google (PDF), Microsoft (PDF), and Yahoo (PDF) yesterday claiming their data protection policies (PDF) flout EU data retention rules.

Under those rules, search engines must anonymize user data after six months. And while most search engines have reduced their data retention periods, none have truly complied with EU regulations. Google (GOOG) keeps user data for nine months. Microsoft (MSFT) keeps it for six, but holds on to software cookies and whatnot for a year beyond that. And Yahoo (YHOO) eliminates user data after 90 days, but only partially.

WASHINGTON (Reuters) - Tech companies such as Apple and Google are hoping the tracks of millions of mobile device users will lead to billions of dollars in revenue.
Kerry: 'Do-Not-Track' Insufficient To Protect Privacy

By Wendy Davis, Wednesday, April 13, 2011

The Kerry-McCain privacy bill, introduced yesterday, would for the first time give users the ability to opt out of behavioral targeting. While regulatory groups have long said that by law they need people opt out of ad targeting and collecting data, the bill is voluntary. The Commercial Privacy contrast, would be mandatory.

Yet it seems like the bill isn’t drawing the attention for what it includes as for what it doesn’t. The proposal doesn’t specifically refer to the issue of a mechanism that would allow users to opt out of tracking at once.

EU Slams Google Over Data Retention

MAY 27, 2010 AT 9:28 AM PT

The privacy practices of the world's largest companies are under fire in Europe again. Europe's data protection agencies want Google (PDF), Microsoft (PDF), and their data protection policies (PDF).

Under those rules, search engines in Europe will be required to store user data for only 12 months. And while most search engines are compliant with European data protection laws, Microsoft (MSFT) keeps it for six, but no longer than 18 months.

However, many EU countries have yet to create laws based on the directive, which was originally legislated in 2009, and it's not clear how aggressively various governments will enforce opt-in laws.

"Confusion and uncertainty" is how Dennis Dayman, chief privacy and security officer at Eloqua—a marketing automation provider that's supplying tools to help Web sites offer data capture choices—described the situation. He noted that what makes things even harder is that requirements vary by country and are not always enforced.

Washington (Reuters) - The law companies such as Apple and Google are hoping the track of tens of millions of mobile device users will lead to billions of dollars in revenue.

Eat Your Cookies: EU Privacy Directive Takes Effect Wednesday

MAY 24, 2011 AT 2:28 PM PT

New European Union privacy regulations that require Web sites to get consent from EU users before tracking them around the rest of the Web will go into effect Wednesday. The directive is aimed at cookies used for targeted advertising, and applies to companies operated in any country.

"Confusion and uncertainty" is how Dennis Dayman, chief privacy and security officer at Eloqua—a marketing automation provider that's supplying tools to help Web sites offer data capture choices—described the situation. He noted that what makes things even harder is that requirements vary by country and are not always enforced.

"Confusion and uncertainty" is how Dennis Dayman, chief privacy and security officer at Eloqua—a marketing automation provider that's supplying tools to help Web sites offer data capture choices—described the situation. He noted that what makes things even harder is that requirements vary by country and are not always enforced.
The concept of “privacy” is amorphous, multifaceted, evolving

- Privacy as an economic property right
  - “Free” media, cloud, security costs
- Privacy as freedom from trespass
  - Civil defense, anti-terrorism, law enforcement
- Privacy as freedom to make choices, without improper influence
  - DRM/piracy, eGov/transparency, public figures
In America, most discussions about “privacy” begin with citing these words:

“Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right ‘to be let alone’....”

“The Right to Privacy”
Harvard Law Review
Louis D. Brandeis & Samuel D. Warren
This was the “invention”: snapshot photography (invented 1888)
Frequency of the words “secrecy” versus “privacy” in books from 1890-2000
To my searching, they were first to make a connection between privacy and technology
This was the “business method”: newspapers

“Instantaneous photographs and newspaper[s] have invaded the sacred precincts of private and domestic life... [they] threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’”
Worth noting as an aside . . .

The invention of the camera was so recent, that there were still many people, even “in various parts of Europe,” who still believed it could steal one’s soul, leading James Frazer to observe in *The Golden Bough* (published in 1922):

“There are persons in the West of Scotland who refuse to have their likenesses taken lest it prove unlucky; and give as instances the cases of several of their friends who never had a day’s health after being photographed.”
“I took out my camera and I was taking pictures and pushing her to clean the poop, but she didn't say anything. She was just looking at her dog and petting it.”

“Miss Kim”

Is this really about privacy?

- She was called “dog poop girl”
- But bloggers sourced her identity through social networks
- Seoul Metropolitan Subway is “public transit”
- She chose to act the way she acted
One Verdict:

“She was in public ... doesn't matter if she was in front of 100 or 1,000,00 people.”

Anonymous blog commenter (quoted by Daniel Solove)
Unforgiving and unrelentless pace of proliferation

“Miss Kim” posts pics on South Korean social media site

South Korean bloggers crowdsource identity

South Korean mainstream press

Popular U.S. blogger blogs the story

BoingBoing picks up story

100s 10,000s 1,000,000s 10,000,000s

The Washington Post
Subway Fracas Escalates Into Test Of the Internet’s Power to Shame
By Jonathan Krim
Thursday, July 7, 2005
Here’s what the “dog poop girl” wrote:

“I know I was wrong, but you guys are so harsh. I regret it, but I was so embarrassed so I just wanted to leave there. I was very irritable because many people looked at me and pushed me to clean the poop. Anyhow, I’m sorry. But, if you keep putting me down on the Internet I will sue all the people and at the worst I will commit suicide. So please don’t do that anymore.”
“I know I was wrong, but you guys are so harsh. I’m regret it, but I was so embarrassed so I just wanted to leave there. I was very irritable because many people looked at me and pushed me to clean the poop. Anyhow, I’m sorry. But, if you keep putting me down on the Internet I will sue all the people and at the worst I will will commit suicide. So please don’t do that anymore.”
She had her person "pirated"

Helpless against "technological" forces, she invoked the protection of "law"
“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Adopted by the United Nations General Assembly on December 10, 1948
“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against arbitrary interference or attacks.”

Adopted by the United Nations General Assembly on December 10, 1948
Legal definition of “arbitrary”

“not based on reason or judgment but on personal will or discretion without regard to rules or standards.”

“founded on prejudice or preference rather than on reason or fact.”

“implies an element of bad faith, and it may be used synonymously with tyrannical or despotic.”


So many (old) boundaries dissolving

Virtual v. Physical World

Authoritarian v. Democratic

Local v. Global

Published Media v. Social Media

Public v. Private

State v. Non-State

Work vs. Personal Life
So many (old) boundaries dissolving
So why is all of this important to the Semantic Web?
Because it forms the basis of a new pairing:
Because it forms the basis of a new pairing:

The Invention(s):
- The “Semantic Web” (and advancements in knowledge discovery and data-mining)

The Business Model:
- “Big Data”
Why now?

Unprecedented access to large amounts of data, leading to sound bite *de jure*:

“more data beats better algorithms”*

and Wired magazine to declare “The End of Science” in its July ’08 issue

*Anand Rajaraman on his Datawocky blog
Explosion of data

According to the Economist, ‘the amount of digital information increases 10X every five years (outpacing available storage).

(From “Data, data everywhere” The Economist February 27, 2010)
But really it’s because access, storage and processing costs are all magnitudes cheaper.
But really it’s because access, storage and processing costs are all magnitudes cheaper

You need a hustler, a designer and a "prodineer."
Sharp contrast to the 1970s through 1990s

Took Donnelly, Polk, etc. 5 years to mash 1970s U.S. Census data (aggregates of 1,500 households) into datasets that were demographically accurate for over 50% of all households.
Today, with networked PCs and mobile devices, “personal data” grew exponentially.
AudienceScience – Behavioral targeting using media consumption to ID segments
ClearSight Interactive - Demographic data matched to 200 million-plus IP addresses

ClearSight Interactive

ClearSight’s Audience Targeting Improves Your Online Advertising:

- Use proven offline data to target millions of online users
- Go beyond cookies...and even replace them
- Heavy-up on your best prospects
- Redeploy impressions you are currently wasting
- Maximize your banner ad campaign’s potential

We don’t make your advertising...we just make it work better.

ClearTarget

ClearTarget offers pre-selected audiences of online users in the top ad spending categories like Financial, Automotive, Healthcare, Travel and more. Using powerful offline predictive data elements for targeted ad serving, we enable advertisers to cut wasteful impression and heavy-up on their best prospects. ClearTarget also enables publishers by creating highly sought-after premium audiences. For both Advertisers and Publishers...more efficient ad campaigns...more sales.

Upcoming Events

OMMA Behavioral
bluecava – Demographic data matched to 125+ million unique device IDs

Most companies do one thing well. We do at least two.

We target online advertising better. And we help fight fraud. With increasing frequency these days companies are saying to us: “Hey, that’s really great technology. I bet I can use it for (fill in the blank with something interesting).”

In the center of BlueCave is our patented way of identifying the unique fingerprint of any Internet connected electronic device. Our universe is big. Like 10 Billion devices in the world big. That’s our sandbox.

Folks use BlueCave for ad targeting because targeting devices is an excellent way to identify and accumulate audiences. BlueCave also helps eliminate online fraud by knowing the identity and behavior of a device. Wouldn’t it be nice to know if that device trying to buy airline tickets from you is really Fred from Fresno or Boris from Bulgaria? BlueCave can help sort it out.
Blue Kai – Shopping activities matched with same user’s media consumption

Data Rules! And We’ve Created the Largest Marketplace for it.

BlueKai’s data-centric approach to audience targeting has made the marketer’s dream of “reaching an audience anytime anywhere” a reality.

We created a marketplace where buyers and sellers trade high-quality targeting data like stocks, while ensuring transparency and control for consumers. Supported by BlueKai’s proprietary platform, this marketplace is an open exchange for all audience data. Most importantly, it’s anchored by BlueKai Intent™, the largest aggregation of in-market shopping data available on the Internet.

BlueKai: Creating a new data economy.
Epsilon/Abacus – Matches people’s online identities with catalog/direct-marketing data
TargusInfo – Matches offline data about users with their online presence
brilig.com – Open platform/exchange for businesses to analyze and share data openly
Sense Networks – Indexes people’s real world habits via mobile and location-based sensors
Ingenix – Provide prescription drug history of patients to health benefits/insurance co’s
face.com - facial recognition technology
Today . . .
This is where all the data comes from
To date, the focus has been on PII and tracking:

- EU Directive – 27 Countries directed to pass new laws about use of cookies
- 2 privacy laws pending in U.S. Congress.
- “Do not track”
- Law suits happening everywhere

But regulators, legislators, courts are struggling with how to apply a “rule of law” . . .
Courts finding it difficult to identify the harm the laws are protecting against:

California court found plaintiffs in a class action against behavioral ad network (Specific Media) failed to articulate how use of “flash cookies” caused them economic injury.

Doubted plaintiffs could, even as a “class action,” meet the $5,000 threshold of injury required.

(Breach of security is a different matter, c.f., RockYou action)
But some are saying that reactive laws that focus on PII will miss the larger dangers:

PEI (Personally Embarrassing Info) Data “Valdez” Changing “business models” and T&Cs De-Anonymization by matching to public datasets “Database of Doom”*

Not so much about actual or perceived economic loss, but rather about fear of what can be “proclaimed from the house-tops” and the right “to be let alone”

California retailer enjoined from asking for "zip code" when customers use a credit card

According to the lawyers explaining their case:

"A lot of the people we talked to felt very uncomfortable giving the ZIP Code but felt they had to. They felt they were in the middle of a transaction and weren't going to tell the sales clerk no."
In “Broken Promise of Privacy,” an influential paper by leading privacy advocate and law professor Paul Ohm cites three examples to illustrate the threat of easy reidentification:

• AOL “Data Valdez”
• 1990 U.S. Census data
• Netflix Personalization Challenge
AOL released the search histories to “embrace the vision of open research”

In August 2006, America Online publicly posted:
-- 20 million search queries
-- sample of 650,000 users
-- covering three months of activity

AOL had deleted member data, IP addresses, etc.
In August 2006, America Online publicly posted:

-- 20 million search queries
-- sample of 650,000 users
-- covering three months of activity

AOL had deleted member data, IP addresses, etc.
Here are some search histories that were stored by AOL

“how to tell your family you’re a victim of incest”

“how to kill your wife”

“depression and medical leave”

“will I be extradited from NY to FL on a DUI charge”

“my baby’s father physically abuses me”

“fear that spouse contemplating cheating”
Yet . . .


Arnold acknowledged her searches which included “mildly embarrassing” queries such as “numb fingers”, “60 single men”, and “dog that urinates on everything.”
Sweeney’s study of 1990 U.S. Census Data

Analysis of the 1990 U.S. Census data showed that 87% of the U.S. Population could be identified uniquely by three non-PII data points:

- Gender
- Birth Date
- 5-digit Zip Code (U.S. Provincial code; e.g., “Beverly Hills 90210”)

Replicated in 2005 study (61% based on 1990 Census and 63% based on 2000 Census)
Sweeney picked an example to demonstrate

- Massachusetts Group Insurance Commission (GIC) released state employees’ records for research purposes.

- GIC removed name, address, social security number, and other “explicit identifiers” but included zip code, gender and birth date.

- Massachusetts Governor William Weld assured the public that GIC had protected patient privacy by deleting all PII.
So Sweeney goes looking for Weld

She purchases voter rolls for Cambridge, Mass for US$20, a public database of name, address, ZIP code, birth date, and gender of every voter.

6 people in Cambridge shared Weld’s birth date, only 3 were men, and only one lived in his ZIP code.

Thus, Sweeney discovered Governor Weld’s health records (diagnoses and prescriptions)
In October 2006, Netflix released de-identified user records for 100 million records of over 500,000 users spanning 1999 to 2005.

• Each record has movie title, 1-5 star movie rating, and date of rating.

• Records represent less than 1/10th of Netflix data in 2005.
Netflix – IMDb mashup

It took Univ of Texas professors Arvind Narayanan and Vitaly Shmatikov just 2 weeks to match Netflix records with public information scraped from IMDb.com to identify 2 subscribers:
Turns out the dataset is very sparse . . .

- 99% of subscribers can be uniquely identified by knowing 8 movie ratings (*with 2 wrong*) and dates of ratings (*with a 14-day error*).

- 68% based on *two ratings and dates* (*with a 3-day error*)

---

**Figure 4. Adversary knows exact ratings and approximate dates.**

From: Arvind Narayanan and Vitaly Shmatikov, *How to Break the Anonymity of the Netflix Prize Dataset* (October 16, 2006)
Even knowing only the movies rated, without the date of ratings . . . 

84% of subscribers can be uniquely identified if 6 out of 8 “long tail” movies (i.e., outside the Top 100/500) “blockbusters”

<table>
<thead>
<tr>
<th>Not in $X$ most rated</th>
<th>$\geq 1$ movie</th>
<th>$\geq 5$</th>
<th>$\geq 10$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X = 100$</td>
<td>100%</td>
<td>97%</td>
<td>93%</td>
</tr>
<tr>
<td>$X = 500$</td>
<td>99%</td>
<td>90%</td>
<td>80%</td>
</tr>
<tr>
<td>$X = 1000$</td>
<td>97%</td>
<td>83%</td>
<td>70%</td>
</tr>
</tbody>
</table>

Figure 8. Adversary knows exact ratings but does not know dates at all.
You don’t have to look far for some “real world” implications:

- U.S. Federal Grand Jury investigation: Pandora’s Android App sending user's birth date, gender, Android ID, and GPS info to advertising companies
- EU may object to Yahoo changing search data retention from 3 to 18 months. Plus, Art. 29 Working Party says U.S. search engines do not meet de-anonymization requirements.
- Netflix sued for retaining movie viewing and rental histories and ratings even after customers cancel their subscriptions.

But how “real” are the harms?
Some powerful anonymization techniques are available, if used correctly:

- **suppression**
  - \( k \)-anonymity: every record projected over quasi-identifiers appears at least \( k \) times, so any data attribute can be linked to \( k \) people at best

- **randomization**
  - introduce randomly incorrect data and then statistically eliminate the “noise” when extracting data

- **encryption-based methods**

- etc.
Piracy is war-like crimes committed in a place not within the jurisdiction of any country.

Pirates are prosecuted as *hostis humani generis* or “enemies of humanity.”
Much of the law on “piracy” was a defense for breaking up State-sponsored monopolies

Hugo Grotius (1583-1654): Lawyer hired by Dutch East India Company to defend the capture (read: piracy) of a Portuguese galleon in 1602 when Spain and Portugal monopolized Asian trade.

“By the Law of Nations, navigation is free to all persons whatsoever ... Every nation is free to travel to every other nation, and to trade with it.”
Grotius’ argument for *Mare Liberum* or *The Freedom of the Seas*:

1. Sovereignty implies private ownership.
2. Private ownership arises from occupation.
3. The sea is limitless. Therefore
4. The sea cannot be occupied, so it cannot be privately owned. Therefore
5. There cannot be sovereignty over the sea.

These words echo what many feel the web should be
Cyberspace consists of transactions, relationships, and thought itself.

We are creating a world that all may enter without privilege or prejudice....

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us.

... from ethics, enlightened self-interest, and the commonweal, our governance will emerge.
So in this conception, who are the pirates? And are “pirates” good or bad?

“Internet is part of public life and thus subject to its laws. Otherwise, we would risk anarchy.”

President Nicolas Sarkozy at G8
“People tell me on the one hand ‘it's great you played such a big role in the Arab spring, but it's also kind of scary because you enable all this sharing and collect information on people.’ But it's hard to have one without the other …. You can't isolate some things you like about the Internet and control other things that you don't.”

Mark Zuckerberg at eG8
“People tell me on the one hand ‘it's great you played such a big role in the Arab spring, but it's also kind of scary because you enable all this sharing and collect information on people.’ But it's hard to have one without the other .... You can't isolate some things you like about the Internet and control other things that you don't.”

Mark Zuckerberg at eG8
With no “versus” to rely-upon, no dissonant “&”s, better to think “uncharted waters”
With no “versus” to rely-upon, no dissonant “&”s, better to think “uncharted waters”
Query: is the “battening down the hatches” approach of “Privacy Advocates” the way?

- Discredited anonymization
- Advocate total ‘opt-in’ consent model or “Privacy Precautionary Principle”*
- Challenge all kinds of uses of data, incl R&D

The problem is where does it end? And does it begin to feel (ironically) Orwellian or smack of censorship?

A Shanghai-based netizen, @littley, tweeted his unfortunate experience: "My SIM card just got deactivated, turning my iPhone to an iPod touch after I texted my dad about Liu Xiaobo winning the Nobel Peace Prize."
Liu Xiaobo and the “empty chair”
China airbrushing Nobel peace prize from internet. Even 'empty chair' isn't safe.

In addition to terms directly tied to jailed Chinese dissident Liu Xiaobo and the Nobel Peace Prize, China's censors now block "empty chair."

Chairman of the Norwegian Nobel Committee Thorbjørn Jagland poses next to the Nobel diploma and Nobel medal placed on the empty chair during the ceremony in Oslo City Hall on Dec. 10, to honor in absentia this years Nobel Peace Prize winner, jailed Chinese dissident Liu Xiaobo.

(Heiko Junge/AP)
To make the science, you need data.

But with privacy advocates scaring consumer and legislators, are we heading towards a “tragedy of the data commons” effect. According to Jane Yakowitz, a Professor at Brooklyn Law School, we are:

- Defensive public guarding anonymized info will lead to a tragedy of commons
- Each will opt out of adding her data to the commons despite benefiting, until the collective benefit degenerates.

How self-defeating when (leg)islators run ahead of the rest of the body
“Technology will move faster than governments, so don't legislate before you understand the consequences.”

Eric Schmidt at G8
March 13, 2009 9:26 AM PDT

**Berners-Lee: Semantic Web will build in privacy**

by Tom Espiner

Web pioneer Tim Berners-Lee says he is making sure the Semantic Web will respect the privacy of online communications and allow people to control who can use their data.
Thank You

Abe Hsuan
AbeHsuanEsq@gmail.com