

We're all peer-to-peer now

Daniel J. Weitzner

MIT Decentralized Information Group

<http://www.w3.org/People/Weitzner.html>

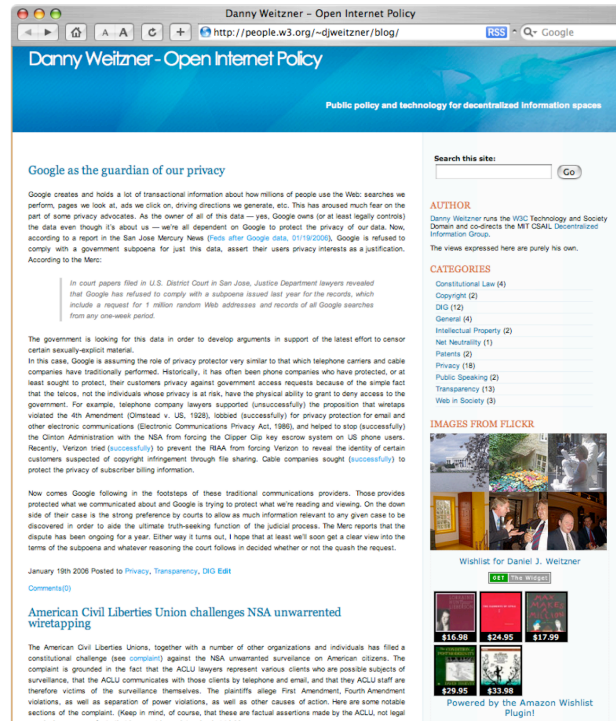


From the 1998 Web -> Web 2.0

Changing usage and traffic patterns



A simple blog page



http://people.w3.org/...

User

Legend

Information Flow ↔

Packet Flow ↔

Network Fees ↔

Links ↔



...from many sources



w3.org



Flickr.com
(Yahoo)

Danny Weitzner - Open Internet Policy

Public policy and technology for decentralized information spaces

Google as the guardian of our privacy

Google creates and holds a lot of transactional information about how millions of people use the Web: searches we perform, pages we look at, ads we click on, driving directions we generate, etc. This has aroused much fear on the part of some privacy advocates. As the owner of all of this data -- yes, Google owns (or at least legally controls) the data even though it's about us -- we're all dependent on Google to protect the privacy of our data. Now, according to a report in the San Jose Mercury News (Feb. after Google data, 01/19/2006), Google is refused to comply with a government subpoena for just this data, assert their users privacy interests as a justification. According to the Merz:

In court papers filed in U.S. District Court in San Jose, Justice Department lawyers revealed that Google has refused to comply with a subpoena issued last year for its records, which include a request for 1 million random Web addresses and records of all Google searches from any one-week period.

The government is looking for this data in order to develop arguments in support of the latest effort to censor certain sexually-explicit material.

In that case, Google is assuming the role of privacy protector very similar to that which telephone carriers and cable companies have traditionally performed. Historically, it has often been phone companies who have protected, or at least sought to protect, their customers privacy against government access requests because of the simple fact that the telcos, not the individuals whose privacy is at risk, have the physical ability to grant to deny access to the government. For example, telephone company lawyers supported (unsuccessfully) the proposition that wiretaps violated the 4th Amendment (Osheski v. US, 1998). Yahoo! supported (unsuccessfully) for privacy protection for email and other electronic communications (Electronic Communications Privacy Act, 1986), and helped to stop (successfully) the Clinton Administration with the NSA from forcing the Clipper Chip key escrow system on US phone users. Recently, Verizon sued (successfully) to prevent the NSA from forcing Verizon to reveal the identity of certain customers suspected of copyright infringement through file sharing. Cable companies sought (successfully) to protect the privacy of subscriber billing information.

Now comes Google following in the footsteps of these traditional communications providers. Those providers protected what we communicated about and Google is trying to protect what we're reading and viewing. On the one side of their case is the strong preference by courts to allow as much information relevant to any given case to be discovered in order to aid the ultimate truth-seeking function of the judicial process. The Merz reports that the dispute has been ongoing for a year. Either way it came out, I hope that at least we'll soon get a clear view into the terms of the subpoena and whatever reasoning the court follows in deciding whether or not to quash the request.

January 19th 2006 Posted to Privacy, Transparency, DIG Edit
Comments

American Civil Liberties Union challenges NSA unwarranted wiretapping

The American Civil Liberties Union, together with a number of other organizations and individuals has filed a constitutional challenge (see [complaint](#)) against the NSA's unwarranted surveillance of American citizens. The complaint is grounded in the fact that the ACLU lawyers represent various clients who are possible subjects of surveillance, that the ACLU communicates with those clients by telephone and email, and that they ACLU staff are therefore victims of the surveillance themselves. The complaint alleges first, amendment, Fourth Amendment violations, as well as separation of power violations, as well as other causes of action. Here are some notable sections of the complaint. (Keep in mind, of course, that these are factual assertions made by the ACLU not legal

Search this site: Go

AUTHOR
Danny Weitzner runs the W3C Technology and Society Domain and co-edits the MIT CSAIL Decentralized Information Group.
The views expressed here are purely his own.

CATEGORIES
Constitutional Law (4)
Copyright (2)
DIG (12)
Genera (4)
Intellectual Property (2)
Net Neutrality (1)
Patents (2)
Privacy (18)
Public Speaking (2)
Transparency (12)
Web in Society (2)

IMAGES FROM FLICKR

Wishlist for Daniel J. Weitzner

Powered by the Amazon Wishlist Plugin

<http://people.w3.org/...>



User

Legend

Information Flow

Packet Flow

Network Fees

Links



Amazon.com

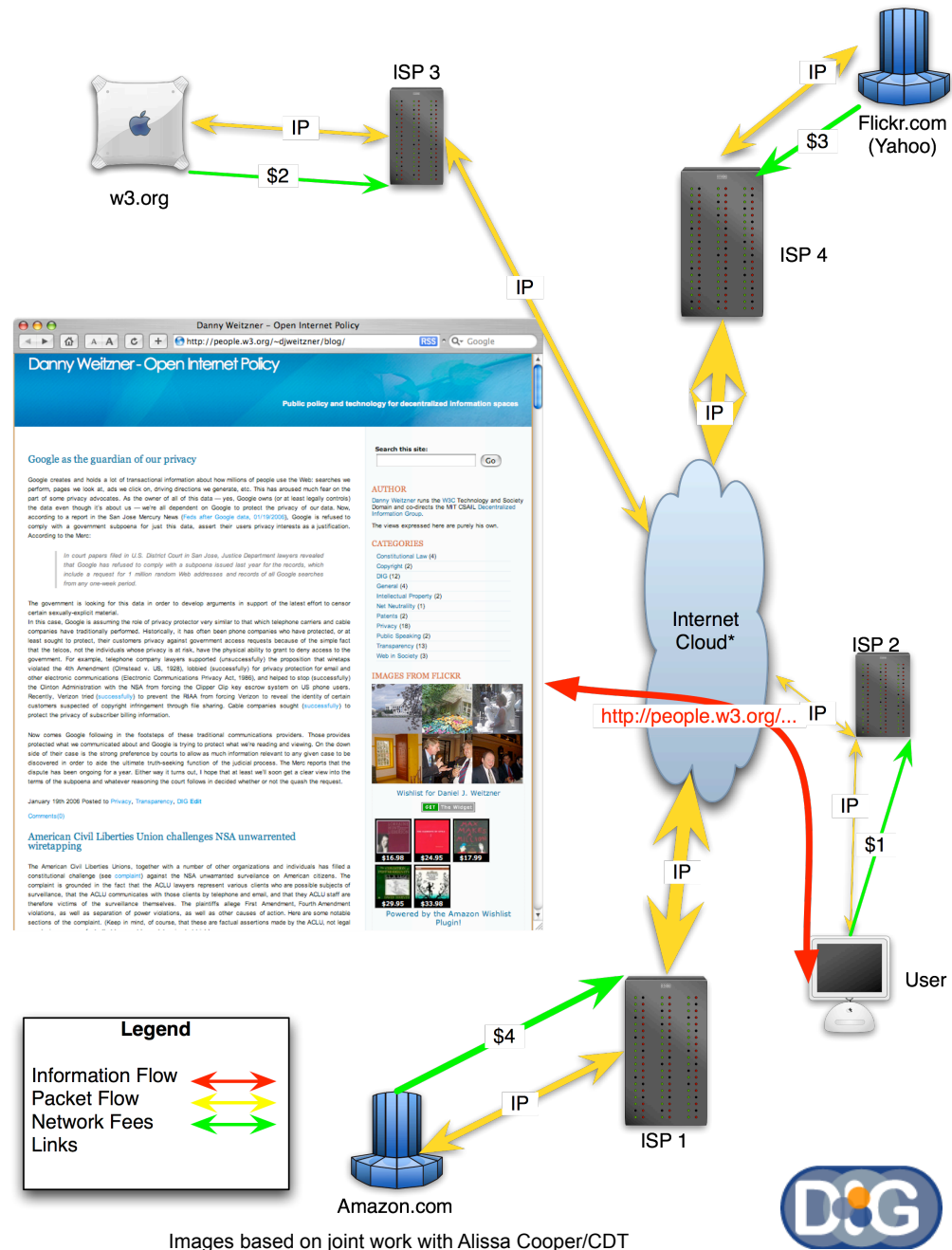


Speakers depend on essential, non-discriminatory features of the Internet

Low/zero transaction costs between speakers & user-audience

- Simple economic model
 - user pays
 - No privity between speaker and user's ISP
- Internet community social compact
 - Common technical protocols
 - Best efforts routing
 - Aggressive network management to curb criminal interference with network operation (spam, DDOS, etc.)

These essential features of the Internet enable open competition, innovation and First Amendment diversity of speakers, but did not arise through market forces alone.



Images based on joint work with Alissa Cooper/CDT