Text Excerpts for Readings #2

Excerpt 1

**COPPA - Children's Online Privacy Protection Act**

from (<http://www.coppa.org/comply.htm>)

The Children's Online Privacy Protection Act, effective April 21, 2000, applies to the online collection of personal information from children under 13. The new rules spell out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online….

An operator must post a link to a notice of its information practices on the home page of its Web site or online service and at each area where it collects personal information from children.

The notice must be clearly written and understandable; it should not include any unrelated or confusing materials. It must state the following information:

* The name and contact information (address, telephone number and email address) of all operators collecting or maintaining children's personal information through the Web site or online service. If more than one operator is collecting information at the site, the site may select and provide contact information for only one operator who will respond to all inquiries from parents about the site's privacy policies. Still, the names of all the operators must be listed in the notice.
* The kinds of personal information collected from children (for example, name, address, email address, hobbies, etc.) and how the information is collected -- directly from the child or passively, say, through cookies.
* How the operator uses the personal information. For example, is it for marketing back to the child? Notifying contest winners? Allowing the child to make the information publicly available through a chat room?
* Whether the operator discloses information collected from children to third parties. If so, the operator also must disclose the kinds of businesses in which the third parties are engaged; the general purposes for which the information is used; and whether the third parties have agreed to maintain the confidentiality and security of the information.
* That the parent has the option to agree to the collection and use of the child's information without consenting to the disclosure of the information to third parties.
* That the operator may not require a child to disclose more information than is reasonably necessary to participate in an activity as a condition of participation.
* That the parent can review the child's personal information, ask to have it deleted and refuse to allow any further collection or use of the child's information. The notice also must state the procedures for the parent to follow.

# Excerpt 2

# Who's watching you online? FTC pushes 'Do Not Track' plan

**By**[**Herb Weisbaum**](http://www.nbcnews.com/id/11620548/)ConsumerMan msnbc.com contributor

From (<http://www.msnbc.msn.com/id/42239031/ns/business-consumer_news/t/whos-watching-you-online-ftc-pushes-do-not-track->)

Bottom of Form

Don't look now, but you're being tracked — some might say stalked — whenever you go online. Information about the sites you visit, the things you buy and the topics you search is used to build a detailed profile about you.  In most cases, this is done without your knowledge or consent.

"The Internet has become a serious threat to our privacy," says Jeff Chester, executive director of the Center for Digital Democracy. By spying on you, companies can learn about your personal finances, religious beliefs, political affiliation, race, ethnic background, even health problems or sexual preferences.

"Most people have no idea this is going on," says Sharon Goott Nissim with the Electronic Privacy Information Center. "Your online profile is being sold on the web. It's kind of crazy and it's not harmless." Right now, this "behavioral tracking" is mainly for marketing purposes, to target the advertising you see online. But the potential for abuse is enormous, since this information can also be used by insurance companies, financial institutions, landlords and prospective employers.

"There are no limits to what types of information can be collected, how long it can be retained, with whom it can be shared or how it can be used," notes Susan Grant, director of consumer protection at the Consumer Federation of America.

…

The industry's solution: an advertising option icon that is now included on some online ads. Click on the icon and you can go to a website that lets you opt out from receiving targeted ads (based on your interests) from some or all of the companies participating in this program.

Consumer advocates find this to be far from adequate. Jeff Chester at the Center for Digital Democracy says it's ludicrous to allow companies that make money by collecting your personal information to be the ones who protect your privacy.

Excerpt 3

## Protecting our kids from online tracking

From (<http://www.commonsensemedia.org/privacy>)

… While the Internet presents tremendous opportunities for entertainment, innovation, and learning, this digital interaction also raises concerns about kids’ and teens’ online privacy and digital footprint. On Thursday, November 14, 2013, a group of bipartisan Members of Congress introduced a bill that enhances online privacy protection for kids and teens, the Do Not Track Kids Act of 2013 (introduced in both the House and Senate). [The act has not yet passed.]

## Here’s How the Do Not Track Kids Act of 2013 Would Protect Kids and Teens Online:

**• Eraser Button:** This bill would require website operators to have an “eraser button” feature that enables users 15 and under to remove content that they posted (to the extent technologically feasible).

**• Opt-in for Behavioral Marketing:** This bill would require companies to get parental consent for children under 13 and consent from teens aged 13-15 in order to send targeted advertising to them.

**• Opt-in for Collection of Personal and Location Information:**This bill would require companies to get parental consent for children under 13 and consent from teens aged 13-15 in order to collect their personal and location information.

**• Digital Marketing Bill of Rights for Teens:** This bill would empower teens aged 13-15 with a new set of protections, including limiting the amount of personal information companies collect and retain about them and promoting security safeguards for their personal information.

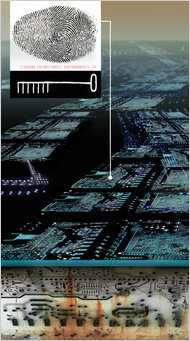
**• Children’s Online Privacy Protection Act (COPPA) Updates:** This bill would reinforce the Federal Trade Commission’s recent updates to the COPPA Rule that strengthen privacy protections for children under 13 in the online, mobile, and social networking ecosystems.

Excerpt 4

# Taking the Mystery Out of Web Anonymity

###### **By**[**JOHN MARKOFF**](http://topics.nytimes.com/top/reference/timestopics/people/m/john_markoff/index.html?inline=nyt-per) **Published: July 3, 2010**

From (<http://www.nytimes.com/2010/07/04/weekinreview/04markoff.html>)

[](javascript:pop_me_up2('http://www.nytimes.com/imagepages/2010/07/04/weekinreview/MARKOFF.html','MARKOFF_html','width=348,height=600,scrollbars=yes,toolbars=no,resizable=yes'))…The Internet affords anonymity to its users — a boon to privacy and freedom of speech. But that very anonymity is also behind the explosion of cybercrime that has swept across the Web.

Can privacy be preserved while bringing a semblance of safety and security to a world that seems increasingly lawless?

Last month, Howard Schmidt, the nation’s cyberczar, offered the Obama administration’s proposal to make the Web a safer place — a “voluntary trusted identity” system that would be the high-tech equivalent of a physical key, a fingerprint and a photo ID card, all rolled into one. The system might use a smart identity card, or a digital credential linked to a specific computer, and would authenticate users at a range of online services.

The idea is to create a federation of private online identity systems. Users could select which system to join, and only registered users whose identities have been authenticated could navigate those systems. The approach contrasts with one that would require a government-issued Internet driver’s license. (Civil liberties groups oppose a government system, fearful that it could lead to national identity cards.)…

Still, the administration’s plan has divided privacy rights activists. Some applaud the approach; others are apprehensive.…

The plan has also been greeted with skepticism by some computer security experts, who worry that the “voluntary ecosystem” envisioned by Mr. Schmidt would still leave much of the Internet vulnerable. They argue that all Internet users should be forced to register and identify themselves, in the same way that drivers must be licensed to drive on public roads.

In the future, he envisions a card that each of us will carry, perhaps equipped with a fingerprint reader, that will in effect be a one-time password system. It will digitally hold all of our different personalities: who we are at work, while playing on-line games, banking and using our smart phones and make it possible for others to be sure we are who we say we are.