**Testimony of**

**Jim Harper**
**Director of Information Policy Studies**
**The Cato Institute**

**to a hearing on**
**Consumer Online Privacy**
**before the**

**Committee on Commerce, Science, and Transportation**
**United States Senate**

**July 27, 2010**

**Executive Summary**

**Privacy is a complicated human interest. People use the word "privacy" to refer to many different things, but its strongest sense is control of personal information, which exists when people have legal power to control information and when they exercise that control consistent with their interests and values.**

**Direct privacy legislation or regulation is unlikely to improve on the status quo. Over decades, a batch of policies referred to as "fair information practices" have failed to take hold because of their complexity and internal inconsistencies.**

**Even modest regulation like mandated privacy notices have not produced meaningful improvements in privacy. Consumers generally do not read privacy policies and they either do not consider privacy much of the time, or they value other things more than privacy when they interact online.**

**The online medium will take other forms with changing times, and regulations aimed at an Internet dominated by the World Wide Web will not work with future uses of the Internet. Privacy regulations that work "too well" may make consumers worse off overall, not only by limiting their access to content, but by giving super-normal profits to today's leading Internet companies and by discouraging consumer-friendly innovations.**

**The "online" and "offline" worlds are collapsing rapidly together, and consumers do not have separate privacy interests for one and the other. Likewise, people do not have privacy interests in their roles as consumers that are separate from their interests as citizens. If the federal government is going to work on privacy protection, it should start by getting its own privacy house in order.**

Chairman Rockefeller, Ranking Member Hutchison, and members of the committee, thank you for inviting me to address your hearing on "Consumer Online Privacy."

My name is Jim Harper, and I am director of information policy studies at the Cato Institute. In that role, I study and write about the difficult problems of adapting law and policy to the challenges of the information age. Cato is a market liberal, or libertarian, think-tank, and I pay special attention to preserving and restoring our nation's founding traditions of individual liberty, limited government, free markets, peace, and the rule of law.

My primary focus is on privacy and civil liberties, and I serve as an advisor to the Department of Homeland Security as a member of its Data Integrity and Privacy Advisory Committee. I am not a technologist, but a lawyer familiar with technology issues. As a former committee counsel in both the House and Senate, I understand lawmaking and regulatory processes related to technology and privacy. I have maintained a web site called Privacilla.org since 2000,[1] cataloguing many dimensions of the privacy issue, and I also maintain an online federal legislative resource called WashingtonWatch.com,[2] which has had over 1.6 million visitors in the last year.

**What is Privacy?**

Your hearing to explore consumer online privacy is welcome. There are many dimensions to privacy, and it is wise to examine all of them, making yourselves aware of the plethora of issues and considerations before turning to legislation or regulation.

People use the word "privacy" to describe many concerns in the modern world, including fairness, personal security, seclusion, and autonomy or liberty. Given all those salutary meanings, everyone wants "privacy," of course. Few concepts have been discussed so much without ever being solidly defined. But confusion about the meaning of the word makes legislation or regulation aimed at privacy difficult.

"Privacy" sometimes refers to the interest violated when a person's sense of seclusion or repose is upended. Telephone calls during the dinner hour,[3] for example, spam emails,[4]

---

[1] http://www.privacilla.org

[2] http://www.washingtonwatch.com Disclosure: WashingtonWatch.com defrays some costs of its otherwise money-losing operation by running Google AdSense ads.

[3] *See* Federal Trade Commission, "Unwanted Telephone Marketing Calls" web page http://www.fcc.gov/cgb/consumerfacts/tcpa.html

[4] The CAN-SPAM Act of 2003 (15 U.S.C. 7701, et seq., Public Law No. 108-187) was intended to remedy the problem of spam, but it remains a huge amount of the SMTP traffic on the Internet. *See* Jim Harper, "CAN-SPAM Didn't – Not By a Long Shot," Cato@Liberty (Nov. 6, 2006) http://www.cato-at-liberty.org/2006/11/06/can-spam-didnt-not-by-a-long-shot/

and—historically—the quartering of troops in private homes[5] undermine privacy and the vaunted "right to be let alone."[6]

For some, it is marketing that offends privacy—or at least targeted marketing based on demographic or specific information about consumers. Many people feel something intrinsic to individual personality is under attack when people are categorized, labeled, filed, and objectified for commerce based on data about them.

This is particularly true when incomplete data fails to paint an accurate picture. The worst denial of personality occurs in the marketing area when data and logic get it wrong, serving inappropriate marketing communications to hapless consumers. A couple who recently lost their baby receives a promotion for diapers or children's toys, for example. Or mail for a deceased parent continues coming long after his or her passing. In the informal sector, communities sometimes attack individuals because of the inaccurate picture gossip paints on the powerful medium of the Internet.[7]

The "privacy" damage is tangible when credit bureaus and other reputation providers paint an incomplete or wrong picture. Employers and credit issuers harm individual consumers when they deny people work or credit based on bad data or bad decision rules.[8]

Other kinds of "privacy" violations occur when criminals acquire personal information and use it for their malign purposes. The scourge of identity theft is a well known "privacy" problem. Drivers Privacy Protection Acts[9] passed in many state legislatures and in the U.S. Congress after actress Rebecca Schaeffer was murdered in 1989. Her stalker got her residence information from the California Department of Motor Vehicles. In a similar notable incident a decade later, Vermont murderer Liam Youens used a data

[5] *See* U.S. Const. amend. III (barring quartering of troops in peacetime).
[6] *Olmstead v. United States*, 277 U.S. 438 (1928) (Brandeis, J, dissenting). Unfortunately, the *Olmstead* case was not about "seclusion" but control of information traveling by wire.
[7] In his book, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET, George Washington University Law School professor Daniel Solove details the story of "Dog Poop Girl," for example, who was selected for worldwide ridicule when a photo of her failing to clean up after her pooch was uploaded and disseminated over the Internet. DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (New Haven: Yale University Press, 2007) pp. 1-4.
[8] Congress passed the Fair Credit Reporting Act (codified at 15 U.S.C. § 1681 et seq.) in 1970 intending to produce fairness in the credit reporting world, which is still an area of difficulty for consumers.
[9] The federal Drivers Privacy Protection Act, Public Law No. 103-322, amended by Public Law 106-69, prohibits the release or use by any State DMV (or officer, employee, or contractor thereof) of personal information about an individual obtained by the department in connection with a motor vehicle record. It sets penalties for violations and makes violators liable on a civil action to the individual to whom the released information pertains.

broker to gather information as part of an Internet-advertised obsession with the young woman he killed.[10]

"Privacy" is also under fire when information demands stand between people and their freedom to do as they please. Why on earth should a person share a phone number with a technology retailer when he or she buys batteries? The U.S. Department of Homeland Security has worked assiduously in what is now called the "Secure Flight" program to condition air travel on the provision of accurate identity information to the government, raising the privacy costs of otherwise free movement.

Laws banning or limiting medical procedures dealing with reproduction offend "privacy" in another sense of the word.[11] There are a lot of privacy problems out there, and many of them blend together.

*Privacy as Control of Personal Information*

The strongest and most relevant sense of the word "privacy," which I will focus on here, though, is its "control" sense—privacy as control over personal information. Privacy in this sense is threatened by the Internet, which is an unusual new medium for many people over the age of eighteen.

In his seminal 1967 book *Privacy and Freedom*, Alan Westin characterized privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[12] A more precise, legalistic definition of privacy in the control sense is: the subjective condition people experience when they have power to control information about themselves and when they have exercised that power consistent with their interests and values.[13] The "control" sense of privacy alone has many nuances, and I will parse them here briefly.

Importantly, privacy is a subjective condition. It is individual and personal. One person cannot decide for another what his or her sense of privacy is or should be.

To illustrate this, one has only to make a few comparisons: Some Americans are very reluctant to share their political beliefs, refusing to divulge any of their leanings or the votes they have cast. They keep their politics private. Their neighbors may post yard signs, wear brightly colored pins, and go door-to-door to show affiliation with a political

[10] *See Remsburg v. Docusearch, Inc.* (N.H. 2003) http://www.courts.state.nh.us/supreme/opinions/2003/remsb017.htm.
[11] *See Griswold v. Connecticut*, 381 U.S. 479 (1965); *Roe v. Wade*, 410 U.S. 113 (1973)
[12] ALAN F. WESTIN, PRIVACY AND FREEDOM, p. 7 (New York: Atheneum 1967).
[13] *See generally*, Jim Harper, "Understanding Privacy—and the Real Threats to It," Cato Policy Analysis No. 520 (Aug. 4, 2004) http://www.cato.org/pub_display.php?pub_id=1652

party or candidate. The latter have a sense of privacy that does not require withholding information about their politics.

Health information is often deemed intensely private. Many people closely guard it, sharing it only with doctors, close relatives, and loved ones. Others consent to have their conditions, surgeries, and treatments broadcast on national television and the Internet to help others in the same situation. More commonly, they relish the attention, flowers, and cards they receive when an illness or injury is publicized. Privacy varies in thousands of ways from individual to individual and from circumstance to circumstance.

An important conclusion flows from the observation that privacy is subjective: government regulation in the name of privacy can be based only on guesses about what "privacy" should look like. Such rules can only ape the privacy-protecting decisions that millions of consumers make in billions of daily actions, inactions, transactions, and refusals. Americans make their highly individual privacy judgments based on culture, upbringing, experience, and the individualized costs and benefits of interacting and sharing information.

The best way to protect true privacy is to leave decisions about how personal information is used to the people affected. Regulatory mandates that take decision-making power away from people will prevent them striking the balances that make them the best off they can be. Sometimes it is entirely rational and sensible to share information.

> Privacy has to do with control of information and its effects on people. To illustrate the complexity of privacy when technology is involved, read "Privacy Advocates Who Don't Understand Privacy" at Appendix I.

At its heart, privacy is a product of autonomy and personal responsibility. Only empowered, knowledgeable citizens can formulate and protect true privacy for themselves, just as they individually pursue other subjective conditions, like happiness, piety, or success.

*The Role of Law*

The legal environment determines whether people have the power to control information about themselves. Law has dual, conflicting effects on privacy: Much law protects the privacy-enhancing decisions people make. Other laws undermine individuals' power to control information.

Various laws foster privacy by enforcing individuals' privacy-protecting decisions. Contract law, for example, allows consumers to enter into enforceable agreements that restrict the sharing of information involved in, or derived from, transactions.

Thanks to contract, one person may buy foot powder from another and elicit as part of the deal an enforceable promise never to tell another soul about the purchase. In addition to explicit terms, privacy-protecting confidentiality has long been an implied term in many contracts for professional and fiduciary services, like law, medicine, and financial services. Alas, legislation and regulation of recent vintage have undermined those protections.[14]

Many laws protect privacy in other areas. Real property law and the law of trespass mean that people have legal backing when they retreat into their homes, close their doors, and pull their curtains to prevent others from seeing what goes on within. The law of battery means that people may put on clothes and have all the assurance law can give that others will not remove their clothing and reveal the appearance of their bodies without permission.

Whereas most laws protect privacy indirectly, a body of U.S. state law protects privacy directly. The privacy torts provide baseline protection for privacy by giving a cause of action to anyone whose privacy is invaded in any of four ways.[15]

The four privacy causes of action, available in nearly every state, are:

- Intrusion upon seclusion or solitude, or into private affairs;
- Public disclosure of embarrassing private facts;
- Publicity that places a person in a false light in the public eye; and
- Appropriation of one's name or likeness.

While those torts do not mesh cleanly with privacy as defined here, they are established, baseline, privacy-protecting law.

Law is essential for protecting privacy, but much legislation plays a significant role in undermining privacy. Dozens of regulatory, tax, and entitlement programs deprive citizens of the ability to shield information from others. You need only look at the Internal Revenue Service's Form 1040 and related tax forms to see that.

*Consumer Knowledge and Choice*

I wrote above about the role of personal responsibility in privacy protection. Perhaps the most important, but elusive, part of privacy protection is consumers' exercise of power

[14] The Gramm-Leach-Bliley Act and federal regulations under the Health Insurance Portability and Accountability Act institutionalized sharing of personal information with government authorities and various "approved" institutions. See 15 U.S.C. §§ 6802(e)(5)&(8); various subsections of 45 C.F.R. 164.512.

[15] Privacilla.org, "The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection," (July 2002) http://www.privacilla.org/releases/Torts_Report.html.

over information about themselves consistent with their interests and values. This requires consumers and citizens to be aware of the effects their behavior will have on exposure of information about them.

Technology and the world of commerce are rapidly changing, and personal information is both ubiquitous and mercurial. Unfortunately, there is no horn that sounds when consumers are sufficiently aware, or when their preferences are being honored. But study of other, more familiar, circumstances reveals how individuals have traditionally protected privacy.

> Consumers' privacy preferences are unpredictable and changing. To see an illustration of this, read about Facebook's "News Feed" in Appendix II.

Consider privacy protection in the physical world. For millennia, humans have accommodated themselves to the fact that personal information travels through space and air. Without understanding how photons work, people know that hiding the appearance of their bodies requires them to put on clothes. Without understanding sound waves, people know that keeping what they say from others requires them to lower their voices.

From birth, humans train to protect privacy in the "natural" environment. Over millions of years, humans, animals, and even plants have developed elaborate rules and rituals of information sharing and information hiding based on the media of light and sound.

Tinkering with these rules and rituals today would be absurd. Imagine, for instance, a privacy law that made it illegal to observe and talk about a person who appeared naked in public without giving the nudist a privacy notice and the opportunity to object. People who lacked the responsibility to put on clothes might be able to sue people careless enough to look at them and recount what they saw. A rule like that would be ridiculous.

The correct approach is for consumers to be educated about what they reveal when they interact online and in business so that they know to wear the electronic and commercial equivalents of clothing.

Of all the online privacy concerns, perhaps the most fretting has been done about "behavioral advertising"—sometimes referred to as "psychographic profiling" to get us really worked up. What is truly shocking about this problem, though, is that the remedy for most of it is so utterly simple: exercising control over the cookies in one's browser.

Cookies are small text files that a web site will ask to place in the memory of computers that visit it. Many cookies have distinct strings of characters in them that allow the web site to "recognize" the computer when it visits the site again. When a single domain places content across the web as a "third party"—something many ad networks do—it

can recognize the same computer many places and gain a sense of the interests of the user.


The solution is cookie control: In the major browsers (Firefox and Internet Explorer), one must simply go to the "Tools" pull-down menu, select "Options," then click on the "Privacy" tab to customize one's cookie settings. In Firefox, one can decline to accept all third-party cookies (shown inset), neutering the cookie-based data collection done by ad networks. In Internet Explorer, one can block all cookies, block all third-party cookies, or even choose to be prompted each time a cookie is offered.[16]

Again, consumers educated about what they reveal when they interact online can make decisions about how to behave that will protect privacy much better—in all online contexts—than consumers unaware of how the world around them works.

**Can Direct Regulation Protect Privacy Better?**

Above, I wrote about how law protects people's privacy-protecting decisions. This unfortunately leaves them with the responsibility of making those decisions. Naturally, most privacy advocates—myself included—believe that people do not do enough to protect their privacy. Consciously or not, people seem to prioritize the short-term benefits of sharing personal information over the long-term costs to their privacy.

This poses the question: Can direct regulation protect consumers privacy better than they can protect themselves?

There is a decades-long history behind principles aimed at protect privacy and related interests, principles that are often put forward as a framework for legislative or regulatory directives.

In the early 1970s, a group called "The Secretary's Advisory Committee on Automated Personal Data Systems" within the Department of Health, Education, and Welfare did an important study of record-keeping practices in the computer age. The intellectual content of its report, commonly known as the "HEW Report,"[17] formed much of the basis of the

[16] These methods do not take care of an emerging tracker known as "Flash cookies" which must be disabled another way, but consumers aware of their ability and responsibility to control cookies can easily meet the growth of Flash cookies. *See* "Flash Player Help" web page, Global Privacy Settings panel, http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager02.html

[17] "Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems," Department of Health, Education, and Welfare [now Department of Health and Human Services] (July, 1973) http://www.aspe.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm

Privacy Act of 1974. The report dealt extensively with the use of the Social Security Number as the issues stood at that time.

The HEW report advocated the following "fair information practices":

- There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for an individual, to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

These things sound wonderful in the abstract, but their relevance, worthiness, and cost-justifications vary widely from circumstance to circumstance.

In 1980, the Organization for Economic Cooperation and Development (OECD) [18] issued similar, if more detailed guidelines. The OECD Guidelines involve eight principles, which in different variations are often touted as "fair information practices" or "fair information practice principles."

They include a "Collection Limitation Principle," a "Data Quality Principle," a "Purpose Specification Principle," a "Use Limitation Principle," a "Security Safeguards Principle," an "Openness Principle," an "Individual Participation Principle," and an "Accountability Principle." The full OECD principles, in their sprawling glory, are reproduced in a footnote below.[19]

---

[18] The OECD consists of bureaucrats from 29 countries that work to coordinate policies with the nominal aim of fostering international trade. The United States is a member of the OECD and the largest funders of its $424 million dollar 2010 budget. *See* Organization for Economic Cooperation and Development, "Member Countries' Budget Contributions for 2010" web page http://www.oecd.org/document/14/0,3343,en_2649_201185_31420750_1_1_1_1,00.html.

[19] 1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, compete and kept up-to-date.

3. Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfilment of those

In a 2000 report, the Federal Trade Commission came out with a relatively briefer list of "fair information practices" (notice, choice, access, and security) and asked Congress for authority to impose them on the businesses of the country,[20] even though a committee convened by the FTC could not reconcile the inherent tensions between access and security.[21] Congress declined to take the FTC's advice.

These examples illustrate one of the problems with the idea of "baseline privacy regulation" for the Internet that has been a consistent call of many for over a decade. There are many good ideas and good practices described in the HEW Report, the OECD Guidelines, and in various other iterations of "fair information practices," but tensions among the principles and variations in their applicability to different circumstances make "FIPs" a poor guide for smart legislating.

"Fair information practices" remain largely aspirational after nearly 40 years, and where they have been implemented, privacy has not blossomed. The principal example is the Privacy Act of 1974, which has done little to give American citizens control over

---

purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Principle 3 except:

- with the consent of the data subject; or
- by the authority of law.

5. Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle: An individual should have the right:

- (a) to obtain from the data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- (b) to have communicated to him, data relating to him
  - within a reasonable time;
  - at a charge, if any, that is not excessive;
  - in a reasonable manner; and
  - in a form that is readily intelligible to him;
- (c) to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and
- (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

8. Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

[20] Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace," (May 2000) http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

[21] *See* FTC Advisory Committee on Online Access and Security , "Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security" (May 15, 2000) http://www.ftc.gov/acoas/

information the government collects. It is shot through with exceptions, and it is largely a paper tiger.

The Fair Credit Reporting Act has guided the development of the credit reporting industry for four decades, while insulating credit bureaus from state tort laws. During that period, the industry has become highly cartelized, consisting of three players (as discussed below, a typical consequence of regulatory barriers to entry). It has failed to innovate and become the reputation and identity service that the world of e-commerce could use. And—most importantly for these purposes—credit reporting is a consumer-unfriendly industry. Rather than working with consumers to develop mutually beneficial personal data repositories, the credit reporting industry serves its financial industry partners first, federal regulators second, and consumers as a rather distant afterthought.

The privacy regulations implemented under the Health Insurance Portability and Accountability Act are sometimes touted as reflecting "fair information practices." (With their breadth, any good data practice is arguably a FIP.) But health privacy has not materialized since Congress shrugged its shoulders and handed the privacy problem to the Department of Health and Human Services.[22] Pre-HIPAA studies showing that patients sometimes avoided treatment due to privacy worries have not been matched by post-HIPAA studies showing that consumers confident of health privacy are getting medical care they would not have gotten.

Fair information practices are widely touted as models for direct regulation that would protect privacy. But the examples we have of FIP-style laws and regulations have not delivered privacy. Privacy protection is hard, and it is not amenable to top-down solutions.

**Keeping it Simple: What About Privacy Notice?**

If the full suite of "fair information practices" is too intricate and internally inconsistent to produce a flowering of privacy across the land, perhaps some minimal privacy regulation would move the ball in the right direction. Mandated privacy notices are widely regarded as a step that would put consumers in a position to protect privacy themselves.

One would think. But they haven't.

A decade ago, market pressure spurred commercial web sites to adopt and publish privacy policies. The FTC found in its 2000 report that 100% of the most popular sites on

[22] *See* Privacilla.org, "Health Privacy in the Hands of Government: The HIPAA Privacy Regulation — Troubled Process, Troubling Results" (April, 2003) http://www.privacilla.org/releases/HIPAA_Report.pdf

the web and 88% of randomly sampled sites had privacy disclosures of some kind.[23] This was in the absence of any regulation requiring notice; it was simply the product of market-based consensus that privacy notice was an appropriate business practice.

However, over the ensuing decade it has become clear that privacy notices do not materially improve consumers' privacy practices. The Federal Trade Commission, other agencies, researchers like Lorrie Faith Cranor at Carnegie Mellon University's "CUPS" laboratory,[24] and others are diligently pursuing strategies to make notices effective at communicating privacy information to consumers in the hope that they will act on that information. But none has yet borne fruit.

The FTC and seven other regulators recently revealed a new, "short" financial privacy notice (required annually of financial services providers by the Gramm-Leach-Bliley Act) that they say "will make it easier for consumers to understand how financial institutions collect and share information about consumers."[25] Perhaps privacy awareness will flourish in the financial services area under this new regime, validating the widely derided privacy notices that clutter Americans' mailboxes. More likely, artificial "notice" will continue to lose currency as a tool for generating consumer focus on privacy.

Nutrition labels, the beloved model for privacy notices, have failed to stem the tide of fat washing over Americans' waistlines. Consumer behavior is difficult to control, as it should be in a free country.

Notice has other challenges. If it ever was, the "online" environment is no longer confined to a series of web pages, of which one could contain a universal privacy policy. The Internet is amenable to endless new protocols and forms of communication, which may defy the idea that there is somewhere for a notice to be located.

Even the growth of handheld devices—an incremental step in comparison to what may come in the future—challenges the idea of notice. Given the very small screen space of many devices, where is a notice to be located? And where is a notice to be located when there isn't a hypertext "link" structure to follow?

A hint of how unsuited privacy notices are to the future of the Internet lies in a dust-up about Google's privacy notice that occurred in mid-2008. A California law passed in

---

[23] *See* Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace," Appendix C, Table 2A (May 2000) http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[24] http://cups.cs.cmu.edu/

[25] Press release, "Federal Regulators Issue Final Model Privacy Notice Form" (Nov. 17, 2009) http://www.cftc.gov/ucm/groups/public/@newsroom/documents/pressrelease/opafinalprivacynoticeform.pdf

2003 requires web sites to have privacy policies linked to from their home pages.[26] At some point, privacy advocates noticed that Google did not have such a link. Access to Google's industry-leading "Privacy Center" was accessible by doing a search on any number of terms or phrases, such as: *What is Google's privacy policy?*

Google, after all, is a search engine. In fact, it is the search engine that augured the decline of the Internet "portal" in favor of more fluid, search-based entrée to the web. Yet the California law requires a portal-style link, something that Google agonized over, being very proud of their very clean home page.[27] Google now has a privacy link on its home page. It has cured its online paperwork violation.

As this story illustrates, Americans are not going on the web through portals any more. Americans are not going "online" sitting at computers looking at web pages any more. There is no end to the protocols that people may use to communicate on the Internet, and a notice regime designed for the World Wide Web so popular in the decade just past will fail to reach people in the decades to come.

**What Does "Online" Mean Anyway? And Why Is It Important?**

It is important to consider changes in technology of a different kind, particularly the vanishing border between "online" and "offline." As I deliver my oral testimony to the committee today, for example, I will be nominally "offline." However, audio and video of my presentation may be streamed live over the Internet or recorded and posted on the committee's web site or elsewhere. Reporters and researchers may take snippets of what I say and weave them into their work, posting those works online.

The phone in my pocket will be signaling its whereabouts (and inferentially mine) to nearby cell towers. Video of me entering, walking around inside, and leaving the Russell building may be captured and stored by the Capitol Police. Should the need arise, they may move this video into permanent storage.

There are privacy consequences from all these things. More than others, I suppose, I knowingly and willingly encounter privacy loss in order to be here and speak to you.

But what is the difference between the privacy consequences of this "offline" behavior and "online" behavior. Why should special privacy protections kick in when one formally

---

[26] *See* Jim Harper, "GOOGLE FAKES COMPLIANCE WITH PRIVACY LAW. OBSCURE BLOGGER DEMANDS INVESTIGATION. DEVELOPING . . ." TechLiberation.com (July 4, 2008) http://techliberation.com/2008/07/04/google-fakes-compliance-with-privacy-law-obscure-blogger-demands-investigation-developing/

[27] *See* Marissa Meyer, "What comes next in this series? 13, 33, 53, 61, 37, 28..." The Official Google Blog (July 3, 2008) http://googleblog.blogspot.com/2008/07/what-comes-next-in-this-series-13-33-53.html.

sits down in front of a computer or uses a handheld device to go "online" if so much of "offline" life means the same thing?

The distinction between online and offline is blurring, and legislation or regulation aimed at protecting consumers "online" could create strange imbalances between different spheres of life. Consumers do not have a set of privacy interests that applies to the "online" world and another set that applies "offline."

To address online privacy alone is to miss the mark. This is not to say that the flesh-and-blood world should have privacy regulations like those that have been dreamed up for the Internet. Rather, privacy on the Internet might better be produced the way it is in the "real" world, by people aware of the consequences of their behavior acting in their own best interests.

**Privacy Regulation Might Also Work "Too Well"**

Consumer privacy legislation and regulation might fail because they miss new protocols or technologies, uses of the Internet that are not web-based, for example. But there is an equally plausible likelihood that privacy regulation works too well, in a couple of different senses.

Privacy regulation that works "too well" would give people more privacy than is optimal, making consumers worse off overall. Consumers have interests not just in privacy, but also in publicity, access to content, customization, convenience, low prices, and so on. Many of these interests are in tension with privacy, and giving consumers privacy at the cost of other things they prefer is not a good outcome.

The dominant model for producing Internet content—all the interaction, commentary, news, imagery, and entertainment that has the Internet thriving—is advertising support. Many of the most popular services and platforms are "free" because they host advertisements directed at their visitors and users. Part of the reason they can support themselves with advertising is because they have good information about users that allow ads to be appropriately targeted. It is a fact that well-targeted ads are more valuable than less-well-targeted ads.

This is important to note: Most web-based businesses do not "sell" information about their users. In targeted online advertising, the business model is generally to sell advertisers *access* to people ("eyeballs") based on their demographics. It is not to sell individuals' personal and contact info. Doing the latter would undercut the advertising business model and the profitability of the web sites carrying the advertising.

If privacy regulation "blinded" sites and platforms to relevant information about their visitors, the advertising-supported model for Internet content would likely be degraded.

Consumers would be worse off—entombed by an excess of privacy when their preferences would be to have more content and more interaction than regulation allows advertising to support.

If the Federal Trade Commission's recommendations for "notice, choice, access, and security" had been fully implemented in 2000, for example, it is doubtful that Google would have had the same success it has had over the last decade. It might be a decent, struggling search engine today. But, unable to generate the kind of income it does, the quality of search it produces might be lower, and it may not have had the assets to produce and support fascinating and useful products like Gmail, Google Maps, Google Docs, and the literally dozens of author products it provides consumers.[28]

Not having these things at our fingertips is difficult to imagine—it is much easier to assume that the Google juggernaut was fated from the beginning—but the rise of Google and all the access to information it gives us was contingent on a set of circumstances that allowed it to target ads to visitors in a highly customized and—to some—privacy-dubious way.

As a thought experiment, imagine taking away Google, Facebook, Apple's suite of consumer electronics (and the app universe that has sprung up within it), and the interactivity that AT&T facilitates. Consumers would rightly howl at the loss of richness to their lives, newly darkened by privacy. And we would all be worse off as the economy and society were starved of access to information.

All this is just to show that trading on personal information can make consumers better off overall. It is not to say that Google or any other company is the be-all and end-all, or that public policy should do anything to "prefer" any company. In fact, the other way that privacy regulation might work "too well" is by giving today's leading firms an advantage against future competitors.

A "barrier to entry" is something that prevents competition from entering a market. Barriers to entry often allow incumbents (like the established companies joining me at the witness table today) to charge higher prices and make greater profits than they otherwise would. Common barriers to entry (fair or unfair) include customer loyalty, economies of scale, control of intellectual property, and network effects, to name a few.

Government regulation can act as a barrier to entry in a few different ways. Aside from direct regulation of entry through licensing or grants of monopoly (issues not relevant here), incumbent firms can comply with regulations at a lower cost per sales unit. With a staff of lawyers already in place, the cost per customer of interpreting and applying any regulation are lower for large firms. Whether regulation is merited and tailored or not,

[28] *See* Wikipedia "List of Google products" page http://en.wikipedia.org/wiki/List_of_Google_products.

small competitors "pay more" to comply with it. Regulation impedes their efforts to challenge established firms.

Established firms can strengthen this dynamic by taking part in crafting legislation and regulation. Their lobbyists, lawyers, and interest-group representatives—the good people gathered at this hearing today—will crowd around and work to protect their clients' interests in whatever comes out of the drafting process, here in Congress and at whatever agency implements any new law. Small, future competitors—unrepresented—will have no say, and new ways of doing business those competitors might have introduced may be foreclosed by regulation congenial to today's winners.

In his paper, *The Durable Internet*,[29] my colleague, Cato adjunct fellow Timothy B. Lee, provides a useful history of how regulatory agencies have historically been turned to protecting the companies they are supposed to regulate. This would occur if the FCC were to regulate Internet service under a "net neutrality" regulation regime. It would occur if a federal agency were tasked with protecting privacy. It appears to have happened with the Minerals Management Service. The dynamic of "agency capture" is a mainstay of the regulatory studies literature.

Returning to the example of Google and the FTC's proposal for comprehensive regulation a decade ago: Had Congress given the FTC authority to impose broad privacy/fair information practice regulations, companies like Microsoft and Yahoo! may have turned the regulations to their favor. Today, the company the produces that most popular operating system might still be the most powerful player, and we might still be accessing the web through a portal. Consumers would be worse off for it.

For all the benefits today's leading companies provide, there is no reason they should not be subjected to as much competition as our public policy can allow. The spur of competition benefits consumers by lowering prices and driving innovations. Privacy regulation might work "too well" for them, locking in competitive advantages that turn away competition and allow them super-normal profits.

Comparisons between existing companies and future competitors are one thing. But a major defect of most proposals for privacy protection are their bald omission of an entire category of privacy threat: governments.

**Privacy for Consumers But Not for Citizens?**

Just as people do not have one set of privacy interests for the online world and one for offline, they do not have one set of privacy interests for commerce and another set for

[29] Timothy B. Lee, "The Durable Internet: Preserving Network Neutrality without Regulation," Cato Policy Analysis No. 626 (Nov. 12, 2008) http://www.cato.org/pub_display.php?pub_id=9775.

government. The privacy protections Americans have as consumers should be made available to them as citizens.

Indeed, given the unique powers of governments—to take life and liberty—Americans should have greater privacy protections from government than they do from private sector entities.

Governments thrive on information about people. Personal information allows governments to serve their citizenry better, to collect taxes, and to enforce laws and regulations. But governments stand in a very different position to personal information than businesses or individuals. Governments have the power to take and use information without permission. And there is little recourse against governments when they use information in ways that are harmful or objectionable.

In the modern welfare state, governments use copious amounts of information to serve their people. A program to provide medical care, for example, requires the government to collect a beneficiary's name, address, telephone number, sex, age, income level, medical condition, medical history, providers' names, and much more.

Governments also use personal information to collect taxes. This requires massive collections of information without regard to whether an individual views it as private: name, address, phone number, Social Security number, income, occupation, marital status, investment transactions, home ownership, medical expenses, purchases, foreign assets. The list is very, very long.

A third use government makes of personal information is to investigate crime and enforce laws and regulations. Governments' ability to do these things correlates directly to the amount of information they can collect about where people go, what they do, what they say, to whom they say it, what they own, what they think, and so on. We rely on government to investigate wrongdoing by examining information that is often regarded as private in the hands of the innocent. It is a serious and legitimate concern of civil libertarians that government collects too much information about the innocent in order to reach the guilty. The incentives that governments face all point toward greater collection and use of personal information about citizens. This predisposes them to violate privacy.

Yet "consumer privacy" bills planned and introduced in the current Congress do nothing to protect Americans' privacy from government. The leading proposals in the House—Rep. Boucher's (D-VA) draft legislation and H.R. 5777, the "BEST PRACTICES Act," introduced by Rep. Rush (D-IL)—simply exclude the federal government from their provisions.

In fairness, there may be jurisdictional reasons for these exemptions, but the hypocrisy would be a little too rank if the federal government were to impose privacy regulations on the private sector while its own profligacy with citizens' information continues.

If there is to be privacy legislation, the U.S. Congress should demonstrate the commitment of the federal government to getting its own privacy house in order. The federal government should practice what it preaches about privacy.

**Conclusion**

Privacy is a complicated human interest, of that there should be no doubt. In this long written testimony I have only begun to scratch the surface of the issues.

People use the word privacy to refer to many different human interests. The strongest sense of the word refers to control of personal information, which exists when people have legal power to control information and when they exercise that control consistent with their interests and values.

Direct privacy legislation or regulation is unlikely to improve on the status quo. Over decades, a batch of policies referred to as "fair information practices" have failed to take hold because of their complexity and internal inconsistencies. In the cases when they have been adopted, such as in the Privacy Act of 1974, privacy has not blossomed.

Even modest regulation like mandated privacy notices have not produced privacy in any meaningful sense. Consumers generally do not read privacy policies and they either do not consider privacy much of the time or value other things more than privacy when they interact online.

The online medium will take other forms with changing times, and regulations aimed at an Internet dominated by the World Wide Web will not work with future uses of the Internet, as we are beginning to see in handheld devices. Privacy regulations that work "too well" may make consumers worse off overall, not only by limiting their access to content, but by giving super-normal profits to today's leading Internet companies and by discouraging consumer-friendly innovations.

It is an error to think that there are discrete "online" and "offline" experiences. Consumers do not have separate privacy interests for one and the other. Likewise, people do not have privacy interests in their roles as consumers, and a separate set of interests as citizens. If the federal government is going to work on privacy protection, the federal government should start by getting its own privacy house in order.

# Appendix I

## Privacy Advocates Who Don't Understand Privacy

In 2006 an engineer working on an experimental WiFi project for Google wrote a piece of code that sampled publicly broadcast data—the information that unencrypted WiFi routers make available by radio to any receiver within range. A year later, this code was included when Google's mobile team started a project to collect basic WiFi network data using Google's Street View cars.

When Google discovered this issue, they stopped running their Street View cars and segregated the data on their network, which they then disconnected to make it inaccessible.[30] Google announced the error to the public and have since been working with European data authorities to try to get rid of it. The European authorities are making them keep it pending their investigations.

Now a U.S. advocacy group, tripping over itself to make this a federal issue, has done more to invade privacy than Google did.

WiFi nodes are like little radio stations. When they are unencrypted, the data they send out can be interpreted fairly easily by whoever receives the radio signals.

Radio signals can travel long distances, and they pass through or around walls and vehicles, people, shrubs and trees. Broadcasting data by radio at the typical signal-strength for a WiFi set-up creates a good chance that it is going to travel outside of one's house or office and beyond one's property line into the street.

For this reason, people often prevent others accessing the information on Wifi networks by encrypting them. That is, they scramble the data so that it is gibberish to anyone who picks it up. (Or at least it takes an enormous amount of computing power to unscramble the signal.) Most people encrypt their WiFi networks these days, which is a good security practice, though it denies their neighbors the courtesy of using a handy nearby Internet connection if they need to.

Even on an unencrypted WiFi network, much sensitive content will be encrypted. Transactions with banks or payments on commerce sites will typically be encrypted by the web browser and server on the other end (the "s" in "https:" indicates this is happening), so their communications are indecipherable wherever they travel.

Given all this, it's hard to characterize data sent out by radio, in the clear, as "private." The people operating these unsecure WiFi nodes may have *wanted* their communications

[30] *See* "WiFi Data Collection: An Update," the Official Google Blog (May 14, 2010) http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html

to be private. They may have *thought* their communications were private. But they were sending out their communications in the clear, by radio—again, like a little radio station broadcasting to anyone in range.

Picking up the data it did using its Street View cars, Google captured whatever it did during the few seconds that the car was in range of the unencrypted WiFi node. The flashes of data would be quite similar to driving past a row of apartments and seeing snippets of life inside whichever apartments had not fully drawn their curtains. Often, there is nothing happening at all. Once in a while, there may be a flicker of something interesting, but it is not tied to any particular identity.

Google never used this useless data. Not a single fact about a single identifiable WiFi user has been revealed. No personal information—much less private information—got any meaningful exposure.

But a U.S. advocacy group seeking to make a federal case of this story tripped over its privacy shoelaces in doing so. Apparently, researchers for this self-described consumer organization looked up the home addresses of Members of Congress. They went to the homes of these representatives, and they "sniffed" to see if there were WiFi networks in operation there. Then they publicized what they found, naming Members of Congress who operate unencrypted WiFi nodes.

If you care about privacy, this behavior is worse than what Google did. In its gross effort to rain attention on Google's misdeed, this group collected information on identifiable individuals—these members of Congress—and put that information in a press release. That is more "stalkerish" and more exposing of personal information than driving past in an automobile picking up with indifference whatever radio signals are accessible from the street.

The behavior of this group is not a privacy outrage. Politicians volunteer to be objects of this kind of intrusion when they decide that they are qualified to run for federal elective office. It simply illustrates how difficult the "privacy" issue is, when a group pulling off a stunt to draw attention to privacy concerns does more harm to privacy than the "wrongdoer" they are trying to highlight.

# Appendix II

## Facebook's "News Feed": Consumers Privacy Interests are Unpredictable and Changing

In September 2006, Facebook—the rapidly growing "social networking" site— added a feature that it called "News Feed" to the home pages of users. News Feed would update each user regularly on their home pages about the activities of their friends, using information that each friend had posted on the site.[31] "News Feed" was met with privacy outrage.[32] In the view of many Facebook users, the site was giving too much exposure to information about them.

But Facebook pushed back. In a post on the Facebook blog titled, "Calm down. Breathe. We hear you,"[33] CEO Mark Zuckerberg wrote:

> This is information people used to dig for on a daily basis, nicely reorganized and summarized so people can learn about the people they care about. You don't miss the photo album about your friend's trip to Nepal. Maybe if your friends are all going to a party, you want to know so you can go too. Facebook is about real connections to actual friends, so the stories coming in are of interest to the people receiving them, since they are significant to the person creating them.

Though Facebook did make some changes, users ultimately found that News Feed added value to their experience of the site. Today, News Feed is an integral part of Facebook, and many users would probably object vociferously if it were taken away.

This is not to say that Facebook is always right or that it is always going to be right. It illustrates how consumers' privacy interests are unsettled and subject to change. Their self-reported interests in privacy may change—and may change rapidly.

The Facebook "News Feed" example is one where consumers looked at real trade-offs between privacy and interaction/entertainment. After balking, they ultimately chose more of the latter.

Consider how well consumers might do with privacy when they are not facing real trade-offs. Consumer polling on privacy generally uses abstract questions to discover consumers' stated privacy preferences. There is little policymaking value in polling

---

[31] *See* "Facebook Gets a Facelift," The Facebook Blog (Sept. 5, 2006) http://blog.facebook.com/blog.php?post=2207967130

[32] *See* Michael Arrington, "Facebook Users Revolt, Facebook Replies" TechCrunch (Sept. 6, 2006) http://techcrunch.com/2006/09/06/facebook-users-revolt-facebook-replies/

[33] "Calm down. Breathe. We hear you," The Facebook Blog (Sept. 5, 2006) http://blog.facebook.com/blog.php?post=2208197130

data.[34] Determining consumers' true interests in privacy and other values is difficult and complex, but it is taking place every day in the rigorous conditions of the marketplace, where market share and profits are determined by companies' ability to serve consumers in the best ways they can devise.

Some economic studies have suggested how much people value privacy.[35] The goal of privacy advocacy should not be to force unwanted privacy protections on a public that does not want them, but to convince consumers to value privacy more.

[34] Jim Harper and Solveig Singleton, "With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us" (June, 2001) http://cei.org/PDFs/with_a_grain_of_salt.pdf

[35] Alessandro Acquisti at Carnegie Mellon University has made a specialty of studying how consumers value privacy. http://www.heinz.cmu.edu/~acquisti/