Privacy and Personal Health Information

Kevin Kawamoto
University of Washington

Follow this and additional works at: http://commons.pacificu.edu/inter03

Recommended Citation

This Article is brought to you for free and open access by the Interface: The Journal of Education, Community and Values at CommonKnowledge. It has been accepted for inclusion in Volume 3 (2003) by an authorized administrator of CommonKnowledge. For more information, please contact CommonKnowledge@pacificu.edu.
Privacy and Personal Health Information

Rights
Terms of use for work posted in CommonKnowledge.

This article is available at CommonKnowledge: http://commons.pacificu.edu/inter03/44
Privacy and Personal Health Information

Posted on September 1, 2003 by Editor

By Kevin Kawamoto <kawamoto@u.washington.edu>

INDEX:

.01 Growing Concerns Over Privacy
.02 Privacy Laws and Policies
.03 Understanding Privacy Policies
.04 Health Information: HIPAA
.05 Protecting the Privacy of Patients' Health Information
.06 Notes

.01 Growing Concerns Over Privacy (return to index)

As increasing amounts of confidential personal information get stored in computerized databases at grocery stores, libraries, video rental outlets, motor vehicle registration divisions (and other government offices), schools, workplaces, telemarketing services, credit rating agencies, financial institutions, health care facilities – you name it! – a parallel and understandable concern over privacy has also increased in society. Many people worry that their personal information will be used in annoying and even nefarious ways. The annoying category includes unwanted telephone solicitations, junk mail (both electronic and hard copy), and other mass marketing nuisances. The nefarious category includes identity theft, discrimination, harassment, and other problems that arise when people use personal information to cause harm.

Privacy is a concept deeply embedded in American society. In common parlance, it is the right to be left alone, to keep the prying eyes of government, businesses, and others out of one’s personal life. That right has never been absolute, but it seems even more tenuous in the Digital Age as so much personal information is stored, organized, accessed, transferred, sold, and evaluated (often without the subject’s knowledge or consent). Web sites routinely collect personal information about consumers through electronic registration forms, sweepstakes and other contests, “cookies” stored on the Web user’s computer, and in other ways. Grocery stores have their “saver club” cards that allow checkout clerks to electronically record customer...
purchases. Credit rating agencies amass personal financial information from a variety of sources to determine a person’s creditworthiness. The list goes on, and people are obviously getting fed up. On June 27, 2003, approximately 735,000 people contacted the Do-Not-Call Registry within 17 hours of its existence to add their names and phone numbers to a registry that would take them off telemarketing lists. The Federal Trade Commission, which spearheaded the program with the Federal Communications Commission, expected 60 million phone numbers to be registered by the end of the first year of the registry’s availability.

The Electronic Privacy Information Center (EPIC) has reviewed numerous public opinion polls over the years and found that a large number of Americans consistently and strongly support “privacy rights in law to protect their personal information from government and commercial entities.” [1] EPIC reports that people want to know when and what kind of personal information is being collected about them, want to give their affirmative consent before that information is gathered and stored, and want to know how that information is being used. They also “want the ability to obtain redress for privacy violations.” [2] Clearly the loss of personal privacy is a top concern among many of those polled.

.02 Privacy Laws and Policies (return to index)

Laws and policies already exist that are supposed to help protect the public against invasion of privacy – electronic or otherwise. Privacy advocates often invoke the Fourth Amendment to the U.S. Constitution to challenge perceived encroachments on privacy. The Amendment states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. [3]

Obviously the authors of this Amendment did not have electronic information in mind when they composed it, but contemporary lawmakers have extended this right to the electronic frontier. The Electronic Communications Privacy Act (ECPA) of 1986, for example, expanded the scope of existing federal wiretap laws to include protection for electronic communications. ConsumerPrivacy.org summarized on its Web site the impact of the ECPA:

- broadens the scope of privileged communications to include all forms of electronic transmissions, including video, text, audio, and data.
- eliminates the requirement that communications be transmitted via common carrier to receive legal protection.
- maintains restrictions on the interception of messages in transmission and adds a prohibition on access to stored electronic communications.
- responds to the Supreme Court’s ruling in Smith v. Maryland that telephone toll records are not private and restricts law enforcement access to transactional information pertaining to users of electronic communication services.
broadens the reach of the Wiretap Act by restricting both government and private access to communications. [4]

Other relevant laws protecting personal information include The Video Privacy Protection Act of 1988, which prohibits video stores from releasing personally identifiable video rental information unless the consumer gives specific consent in writing. Police need to obtain and present a valid warrant or court order to get personally identifiable video rental information from video stores. These stores are required to destroy rental records no longer than one year after an account is terminated. The Fair Credit Reporting Act allows consumers to find out if their credit information has been used against them and what information is contained in their personal credit report. By having access to their report, consumers can see whether their credit information is accurate and, if not, dispute the inaccuracies. They can also find out who has requested the information within a certain time period. The Family Educational Rights and Privacy Act (FERPA), enacted by Congress in 1974, protects the privacy of student education records at institutions that receive applicable federal funding. It gives students 18 and older, and the parents of students under 18, the right to review certain education records, request corrections if inaccuracies seem present, and request that details considered "public" or "directory" information not be released publicly. (All of these laws are much more complex than stated here and should be researched further if one is interested in getting an in-depth understanding of federal legislation involving privacy.)

These and other laws attempt to protect privacy, and more are sure to be created in the years to come as lawmakers deal with problems such as cybercrime, cyberterrorism, online advertising, e-commerce, e-mail spamming, workplace rights of computer users, and so forth. Children also present a special concern for lawmakers. The Children’s Online Privacy Protection Act (COPPA) and Protection of Children from Sexual Predators Act are designed to protect children from exploitive or predatory behavior. Typically laws and policies regarding electronic information are reactive, however, and take time to catch up with rapid technological advances and abuses. Creating laws and policies to protect privacy requires considerable thoughtfulness and even-handedness. At the extreme, such laws could impede people’s abilities to access information, including the news media’s ability to function as a reporter of current events and watchdog of government. The balancing act between protecting personal privacy and ensuring freedom of information can be difficult to sustain.

Another layer of complexity, especially since September 11, 2001, is the federal government’s covert use of surveillance technology to monitor domestic and transborder communications. The full impact of the U.S. PATRIOT Act on privacy is a question ripe for analysis. Critics of these technologies and related activities believe the federal government and law enforcement agencies are eroding civil liberties, including privacy, under the banner of national security. Advocates of these technologies believe that in times of war – or protracted threats of terrorism – some civil liberties must be compromised in the interest of domestic safety. These debates will no doubt continue for years down the road.

.03 Understanding Privacy Policies (return to index)
Increasingly, businesses are explaining their privacy policies to customers via direct mailings and
on their Web sites. Some of these policy explanations are helpful; others are legalistic and tedious
to read, as if the entire policy was intentionally written in fine print (literally and metaphorically) to
discourage comprehension. To the extent that businesses and government agencies explain their
privacy policies in a way that is comprehensible to the average online consumer, these attempts
at transparency can be viewed as a positive development. If they are convoluted and user-hostile,
they should be viewed as perfunctory exercises meant to give the illusion of transparency
but actually serving to confuse the consumer about the business’s real intentions.

Before divulging any personal information over the phone, on the Web, in person, through the
mail, or by any other medium, savvy consumers should have a good idea about how this
information will be used. Here are some questions that should be answered by the information
gatherer’s privacy policy in clear and precise terms:

- Why is your organization collecting my personal information?
- Does your organization disclose, share, or sell personally identifiable information (e.g.,
  name, address, telephone number, e-mail, and so forth) that it collects from its customers?
- If yes, to whom does it disclose, share, or sell this information? (If the organization says that
  it shares your information only with “affiliated organizations,” who are these so-called
  affiliated organizations?)
- Will the organization use personally identifiable information for future marketing purposes?
  Will I be added to an e-mail mailing list? What other forms of solicitation can I expect to
  receive?
- Can this privacy policy be changed in the future? Will I be notified of changes?
- How is my personal information protected?
- Did you deposit a “cookie” on my computer? How will the information that you collect from
  that cookie be used?
- Can I block the cookies and still access your site?
- Can I review the information about me and make corrections if necessary?
- Can I “opt out” from having my personal information collected and/or released?
- Is there a Web site I can visit or phone number I can call to unsubscribe from mailing or
  telemarketing lists? Who can I contact if I have questions or complaints?

It is unlikely you will get answers to all of these questions, but you should be suspicious of
organizations that are unwilling to address any of these questions. Read the “fine print,” if there is
any, and see what it says. Organizations with ethical privacy policies should be proud to publicize
them in clear and straightforward language.

.04 **Health Information: HIPAA** (return to index)

The computerization of personal medical records is a growing and irreversible phenomenon, one
that involves complex information systems that can digitally store patient histories, lab results,
prescription information, insurance and other financial details, radiological images, inter-physician
consultations, and a cornucopia of other health data about an individual. Arguably, a system of electronic record keeping of personal health information has substantial advantages over the traditional manila folder and circular file method of storing patient data. Electronic records take up less physical space, for one thing. But they also have clear benefits for enhanced patient care. Data can be centralized so that if a patient consults with several health care providers, each of them can access the same information as the other, and add any new information to the same electronic patient record. A series of paper files, on the other hand, can get messy and disorganized, not to mention lost (in part or entirely). Electronic files can be set up in such a way that even voluminous amounts of patient information can be stored and retrieved in an efficient manner. Health care providers can exchange pertinent information with health insurance companies to make sure that timely payments are made for services rendered. The flood of paper forms can be reduced to a stream of bits and bytes from one health-related entity to another.

But if each health care institution and insurance company uses its own particular information system and computer protocols, the electronic communication among entities has the potential to be faulty and chaotic. Consistent technical and procedural standards among various health-related organizations would facilitate the exchange of electronic health information. This was one of the goals of the federal government when it began formulating policies and legislation that would mandate such standards. However, along with this mandate came a strong provision to protect patient privacy, the part of the legislation that became known as the “Privacy Rule” of HIPAA.

What is HIPAA?

On April 14, 2003, U.S. health care providers were supposed to be in compliance with a federal law designed, in part, to protect patients’ personal health information. The law is known as HIPAA, or Health Insurance Portability and Accountability Act of 1996, and every health care provider in the country is likely to be very familiar with its requirements by now.

Among other things, HIPAA imposes strict rules on the release of protected health information or PHI. Violators can incur large fines and/or prison time for non-compliance with HIPAA privacy rules, depending on the intent and nature of the violation. On the high end of the penalties, violators can be fined up to $250,000 and imprisoned for ten years. Both civil and criminal penalties can be imposed. It is important, then, for all people who deal with protected health information to know about HIPAA and carefully adhere to its rules.

HIPAA was designed to achieve at least two major goals. One was to simplify electronic transaction of health information among health care providers (such as hospitals), insurers, and health care clearinghouses (e.g., third parties that translate and transmit data from health care providers to insurers). This simplification process would be accomplished through the standardization of electronic transfer of protected health information for financial and administrative purposes. This process is supposed to help improve the effectiveness and
efficiency of the health care system, as well as bring administrative costs down.

The complete text of this Public Law (104-91) can be accessed on the Department of Health and Human Services Web site, http://privacyruleandresearch.nih.gov/pr_02.asp. Those interested in health information privacy should read the entire legal document. Here is the part that pertains specifically to the creation of "national standards to protect the security and privacy of information," also known as the Privacy Rule:

HIPAA became law in 1996 (Public Law 104-191). Subtitle F of Title II of HIPAA, entitled "Administrative Simplification," requires the Secretary of HHS to adopt national standards for certain information-related activities of the health care industry. The purpose of subtitle F is to improve the Medicare program under title XVIII of the Social Security Act ("Act"), the Medicaid program under title XIX of the Act, and the efficiency and effectiveness of the health care system, by mandating the development of standards and requirements to enable the electronic exchange of certain health information. Section 262 of subtitle F added a new Part C to Title XI of the Act. Part C (42 U.S.C. 1320d-1320d-8) requires the Secretary to adopt national standards for certain financial and administrative transactions and various data elements to be used in those transactions, such as code sets and certain unique health identifiers. Recognizing that the industry trend toward computerizing health information, which HIPAA encourages, may increase the access to that information, the statute also requires national standards to protect the security and privacy of the information. [5]

HIPAA has, in effect, created a national standard for dealing with personal health information. By April 14, 2003, all personnel who come into contact with this kind of information should have been trained about proper handling procedures. Media relations staff and medical personnel should have been aware of what kind of information can be released about patients to a journalist and under what conditions. (The short answer is, “Not much,” at least not without a signed consent form from the patient to release more than the minimal allowable information.) A number of states and health care institutions had their own laws or policies that already adequately addressed relevant privacy concerns, or offered an even higher level of privacy protection than HIPAA does. If those policies do, in fact, offer higher levels of privacy protection, they can remain in effect.

Because of the monumental importance of HIPAA to the field of health informatics [7] where confidential patient information is concerned, this column concludes with a detailed explanation of HIPAA’s patient privacy protection rules. The text is taken verbatim from the U.S. Department of Health and Human Services Fact Sheet on HIPAA, which was released on April 14, 2003. [6] No doubt it is not the last word on electronic information and privacy. It is, rather, the kind of legislation one might expect to find arising in the future when the benefits of information technology raise concerns about personal privacy.

.05 Protecting the Privacy of Patients' Health Information (return to index)
Overview: The first-ever federal privacy standards to protect patients’ medical records and other health information provided to health plans, doctors, hospitals and other health care providers took effect on April 14, 2003. Developed by the Department of Health and Human Services (HHS), these new standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed. They represent a uniform, federal floor of privacy protections for consumers across the country. State laws providing additional protections to consumers are not affected by this new rule.

Congress called on HHS to issue patient privacy protections as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA included provisions designed to encourage electronic transactions and also required new safeguards to protect the security and confidentiality of health information. The final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., enrollment, billing and eligibility verification) electronically. Most health insurers, pharmacies, doctors and other health care providers were required to comply with these federal standards beginning April 14, 2003. As provided by Congress, certain small health plans have an additional year to comply. HHS has conducted extensive outreach and provided guidance and technical assistant to these providers and businesses to make it as easy as possible for them to implement the new privacy protections. These efforts include answers to hundreds of common questions about the rule, as well as explanations and descriptions about key elements of the rule. These materials are available at http://www.hhs.gov/ocr/hipaa.

Patient Protections. The new privacy regulations ensure a national floor of privacy protections for patients by limiting the ways that health plans, pharmacies, hospitals and other covered entities can use patients’ personal medical information. The regulations protect medical records and other individually identifiable health information, whether it is on paper, in computers or communicated orally. Key provisions of these new standards include:

Access To Medical Records. Patients generally should be able to see and obtain copies of their medical records and request corrections if they identify errors and mistakes. Health plans, doctors, hospitals, clinics, nursing homes and other covered entities generally should provide access these records within 30 days and may charge patients for the cost of copying and sending the records.

Notice of Privacy Practices. Covered health plans, doctors and other health care providers must provide a notice to their patients how they may use personal medical information and their rights under the new privacy regulation. Doctors, hospitals and other direct-care providers generally will provide the notice on the patient’s first visit following the April 14, 2003, compliance date and upon request. Patients generally will be asked to sign, initial or otherwise acknowledge that they received this notice. Health plans generally must mail the notice to their enrollees by April 14 and again if the notice changes significantly. Patients also may ask covered entities to restrict the use or disclosure of their information beyond the practices included in the notice, but the covered entities would not have to agree to the changes.
**Limits on Use of Personal Medical Information.** The privacy rule sets limits on how health plans and covered providers may use individually identifiable health information. To promote the best quality care for patients, the rule does not restrict the ability of doctors, nurses and other providers to share information needed to treat their patients. In other situations, though, personal health information generally may not be used for purposes not related to health care, and covered entities may use or share only the minimum amount of protected information needed for a particular purpose. In addition, patients would have to sign a specific authorization before a covered entity could release their medical information to a life insurer, a bank, a marketing firm or another outside business for purposes not related to their health care.

**Prohibition on Marketing.** The final privacy rule sets new restrictions and limits on the use of patient information for marketing purposes. Pharmacies, health plans and other covered entities must first obtain an individual’s specific authorization before disclosing their patient information for marketing. At the same time, the rule permits doctors and other covered entities to communicate freely with patients about treatment options and other health-related information, including disease-management programs.

**Stronger State Laws.** The new federal privacy standards do not affect state laws that provide additional privacy protections for patients. The confidentiality protections are cumulative; the privacy rule will set a national “floor” of privacy standards that protect all Americans, and any state law providing additional protections would continue to apply. When a state law requires a certain disclosure — such as reporting an infectious disease outbreak to the public health authorities — the federal privacy regulations would not preempt the state law.

**Confidential communications.** Under the privacy rule, patients can request that their doctors, health plans and other covered entities take reasonable steps to ensure that their communications with the patient are confidential. For example, a patient could ask a doctor to call his or her office rather than home, and the doctor’s office should comply with that request if it can be reasonably accommodated.

**Complaints.** Consumers may file a formal complaint regarding the privacy practices of a covered health plan or provider. Such complaints can be made directly to the covered provider or health plan or to HHS’ Office for Civil Rights (OCR), which is charged with investigating complaints and enforcing the privacy regulation. Information about filing complaints should be included in each covered entity’s notice of privacy practices. Consumers can find out more information about filing a complaint at [http://www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa) or by calling (866) 627-7748.

**Health Plans and Providers.** The privacy rule requires health plans, pharmacies, doctors and other covered entities to establish policies and procedures to protect the confidentiality of protected health information about their patients. These requirements are flexible and scalable to allow different covered entities to implement them as appropriate for their businesses or practices. Covered entities must provide all the protections for patients cited above, such as providing a notice of their privacy practices and limiting the use and disclosure of information as
required under the rule. In addition, covered entities must take some additional steps to protect patient privacy:

**Written Privacy Procedures.** The rule requires covered entities to have written privacy procedures, including a description of staff that has access to protected information, how it will be used and when it may be disclosed. Covered entities generally must take steps to ensure that any business associates who have access to protected information agree to the same limitations on the use and disclosure of that information.

**Employee Training and Privacy Officer.** Covered entities must train their employees in their privacy procedures and must designate an individual to be responsible for ensuring the procedures are followed. If covered entities learn an employee failed to follow these procedures, they must take appropriate disciplinary action.

**Public Responsibilities.** In limited circumstances, the final rule permits — but does not require — covered entities to continue certain existing disclosures of health information for specific public responsibilities. These permitted disclosures include: emergency circumstances; identification of the body of a deceased person, or the cause of death; public health needs; research that involves limited data or has been independently approved by an Institutional Review Board or privacy board; oversight of the health care system; judicial and administrative proceedings; limited law enforcement activities; and activities related to national defense and security. The privacy rule generally establishes new safeguards and limits on these disclosures. Where no other law requires disclosures in these situations, covered entities may continue to use their professional judgment to decide whether to make such disclosures based on their own policies and ethical principles.

**Equivalent Requirements For Government.** The provisions of the final rule generally apply equally to private sector and public sector covered entities. For example, private hospitals and government-run hospitals covered by the rule have to comply with the full range of requirements.

**Outreach and Enforcement.** HHS' Office for Civil Rights (OCR) oversees and enforces the new federal privacy regulations. Led by OCR, HHS has issued extensive guidance and technical assistance materials to make it as easy as possible for covered entities to comply with the new requirements. Key elements of OCR's outreach and enforcement efforts include:

**Guidance and technical assistance materials.** HHS has issued extensive guidance and technical materials to explain the privacy rule, including an extensive, searchable collection of frequently asked questions that address major aspects of the rule. HHS will continue to expand and update these materials to further assist covered entities in complying. These materials are available at [http://www.hhs.gov/ocr/hipaa/assist.html](http://www.hhs.gov/ocr/hipaa/assist.html).

**Conferences and seminars.** HHS has participated in hundreds of conferences, trade association meetings and conference calls to explain and clarify the provisions of the privacy
regulation. These included a series of regional conferences sponsored by HHS, as well as many held by professional associations and trade groups. HHS will continue these outreach efforts to encourage compliance with the privacy requirements.

**Information line.** To help covered entities find out information about the privacy regulation and other administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996, OCR and HHS' Centers for Medicare & Medicaid Services have established a toll-free information line. The number is (866) 627-7748.

**Complaint investigations.** Enforcement will be primarily complaint-driven. OCR will investigate complaints and work to make sure that consumers receive the privacy rights and protections required under the new regulations. When appropriate, OCR can impose civil monetary penalties for violations of the privacy rule provisions. Potential criminal violations of the law would be referred to the U.S. Department of Justice for further investigation and appropriate action.

**Civil and Criminal Penalties.** Congress provided civil and criminal penalties for covered entities that misuse personal health information. For civil violations of the standards, OCR may impose monetary penalties up to $100 per violation, up to $25,000 per year, for each requirement or prohibition violated. Criminal penalties apply for certain actions such as knowingly obtaining protected health information in violation of the law. Criminal penalties can range up to $50,000 and one year in prison for certain offenses; up to $100,000 and up to five years in prison if the offenses are committed under “false pretenses”; and up to $250,000 and up to 10 years in prison if the offenses are committed with the intent to sell, transfer or use protected health information for commercial advantage, personal gain or malicious harm.

.06 **NOTES** (return to index)


[2] Ibid.


Past columns in this series help explain the concept and practice of health informatics. They can be accessed through the links below:

“Health Information Online Abundant and Varied"

“Teaching Students About Cyberhealth Information”
http://bcis.pacificu.edu/journal/2003/01/kawamoto.php

“Older Adults and the Internet”
http://bcis.pacificu.edu/journal/2003/02/kawamoto.php

“Computer Technology in Health Care Settings”
http://bcis.pacificu.edu/journal/2003/04/kawamoto.php

This entry was posted in Uncategorized by Editor. Bookmark the permalink [http://bcis.pacificu.edu/interface/?p=2798].

18 thoughts on "PRIVACY AND PERSONAL HEALTH INFORMATION"

need for speed world boost hack 2013
on January 30, 2014 at 3:23 AM said:

Is information currently available electronically in the system being reproduced by hand on paperwork. They are both from the drawing board racing machines built to accelerate at rates that will put all but a jet fighter to shame. good top end, a quick shifting gear box, great handling and just plain fun, but this car can sure be a handful.

nfs world boost hack
on January 30, 2014 at 10:21 AM said:

Need for Speed: Hot Pursuit is a 2010 racing video game being developed. 2003 Ford Focus ZX3: FWD, 130 hp, 5300 rpm, 135 lbs. good top end, a quick shifting gear box, great handling and just plain fun, but this car can sure be a handful.
Clementina Frago  
on January 30, 2014 at 6:14 PM said:

Thank you a bunch for sharing this with all of us you really recognize what you are talking approximately! Bookmarked. Kindly also discuss with my web site =). We can have a link exchange agreement between us!

best masticating juicer  
on January 31, 2014 at 7:04 AM said:

Wow, that’s what I was exploring for, what a material! present here at this webpage, thanks admin of this website.

top eleven football manager cheats  
on January 31, 2014 at 12:26 PM said:

Bringing with him his football gifts, European style and foreign signings and a much-needed discipline to the Club, Arsenal achieved great triumph under him. Even cooler, MFL offers up to 28 different positions, including the ability to draft and play individual defensive players, or a team’s defensive backfield or defensive line together. I know it’s just a game, but if you want to win doing a little homework is a necessity.

chainsaw reviews  
on February 1, 2014 at 5:29 AM said:

What i do not realize is actually how you’re now not actually a lot more smartly-appreciated than you might be now. You’re very intelligent. You already know therefore considerably with regards to this subject, produced me in my view consider it from a lot of varied angles.

Its like men and women aren’t fascinated until it’s something to
accomplish with Woman gaga! Your individual stuffs excellent.
Always care for it up!

exercise bike reviews
on February 3, 2014 at 6:51 PM said:

You actually make it appear so easy together with your presentation but I find this matter to be really one thing that I feel I’d never understand.
It kind of feels too complicated and extremely wide for me.
I am taking a look forward for your subsequent put up,
I will attempt to get the cling of it!

vacuum sealer reviews
on February 3, 2014 at 7:45 PM said:

I used to be suggested this website through my cousin.
I’m not sure whether or not this post is written through him as nobody else realize such precise approximately my problem.
You are incredible! Thank you!

espresso machine reviews
on February 3, 2014 at 9:19 PM said:

Howdy! I’m at work browsing your blog from my new iphone 4!
Just wanted to say I love reading through your blog and look forward to all your posts! Keep up the fantastic work!

best home gym
on February 3, 2014 at 10:31 PM said:
I was suggested this web site by my cousin. I am not sure whether this post is written by him as no one else know such detailed about my trouble.

You are wonderful! Thanks!

infrared grill reviews
on February 3, 2014 at 10:37 PM said:

I’m extremely inspired together with your writing talents and also with the structure for your blog.

Is this a paid topic or did you modify it your self? Anyway stay up the excellent quality writing, it is rare to see a great blog like this one nowadays..

best humidifier
on February 3, 2014 at 11:37 PM said:

Good web site you have got here.. It’s difficult to find high-quality writing like yours these days.
I seriously appreciate people like you! Take care!!

clothes steamer reviews
on February 4, 2014 at 2:08 AM said:

I have fun with, lead to I discovered exactly what I used to be having a look for. You have ended my 4 day lengthy hunt!

God Bless you man. Have a great day. Bye
If some one wishes expert view on the topic of running a blog afterward i advise him/her to pay a quick visit this web site, Keep up the pleasant work.

dating
on February 4, 2014 at 10:16 AM said:

Great blog correct here! Additionally your internet site loads up extremely fast! What host are you the usage of? Can I get your associate link on your host? I wish my web site loaded up as easily as yours lol

nigeria entertainment news
on February 4, 2014 at 10:27 AM said:

i had to complete was article many comments on the houseparty site, invite

nigeria entertainment news
on February 4, 2014 at 10:35 AM said:

A individual basically help to create a lot content I would state. This really is the first time I frequented your site article and as much as now? I amazed of the analysis you created to generate this real write-up extraordinary. Beneficial task!

best electric tea kettle
on February 4, 2014 at 10:11 PM said:

Hello there! I could have sworn I’ve been to this website before but after checking through some of the post I realized it’s new to me. Anyways, I’m definitely glad I found it and I’ll be book-marking and checking back frequently!