



Broad Coalition Says Consumer Role Is Key to Improving Health and Health Care

PRNEWSWIRE-USNEWSWIRE

NEW YORK, June 25 - The future of health care should encourage expanded use of information tools to help consumers better manage their health, 56 diverse organizations said today as they embraced a framework for personal health information access and privacy.

"Consumers need to be full participants in modern health information tools and services to help them prevent illness, communicate better with clinicians, understand costs and treatment options, make better health decisions, and take better care of loved ones," the group said in a joint statement.

"Health reform requires putting the power of information at the fingertips of 300 million consumers," said Zoe Baird, president of the Markle Foundation, which convened the group. "If we do this right, consumers will contribute to a health care system that rewards quality, slows an unsustainable spiral of costs, and protects the privacy of sensitive information."

The recently enacted American Recovery and Reinvestment Act establishes billions of dollars in incentives for clinicians and hospitals to use health information technology, including electronic health records (EHRs). The law also clarifies that individuals have the right to receive copies of personal health information from EHRs in electronic formats and authorize their information to be stored in a service of the individual's choosing.

"In the age of the Internet, there is vast potential for consumers to connect online to new services to make their lives easier and healthier," said Carol Diamond, MD, MPH, chair of Markle Connecting for Health, which convened the group. "Providing consumers with electronic access to their information should be one of the things that the health IT incentives stimulate, so that many services may flourish by using information according to the individual's needs and wishes."

Deven McGraw, director of the Health Privacy Project for the Center for Democracy and Technology, said: "Sound policies are key to public trust -- without which we will not see the benefits of health IT investments. Consumers and clinicians will not participate if they fear information will not be protected."

Source: <http://www.earthtimes.org/articles/show/broad-coalition-says-consumer-role,873753.shtml>

Inside this issue:

Heath IT	2
Privacy and Security	4
New Reports and Papers	6
Points of View	11
Internet Governance	16
Book Notice	20

FIGURES OF THE WEEK

- A new study finds that 86 percent of consumers believe that profitable businesses can address social issues. The poll, conducted May 18-28, 2009, among a sample of 511 consumers and 320 marketing professionals nationwide, highlights the current state of key consumer perceptions in the area of corporate social responsibility. The joint research poll, conducted by Waggener Edstrom Worldwide (WVE), a global multiservice communications agency, and RT Strategies, a bipartisan public affairs opinion research and polling organization, finds that nearly half of the consumers surveyed and over half of the marketing professionals surveyed rank the economy as their No. 1 concern. Despite growing concerns about corporate corruption, economic recession and global instability, consumers and marketing professionals believe companies can make a positive change in society through the products and services they sell.
- The market of mobile financial services to poor people in emerging markets will surge from nothing to \$5 billion in 2012, U.S.-based microfinance policy and research center CGAP said on Monday. The market began in early 2007 with a launch of Safaricom's M-PESA in Kenya, which has attracted 6.5 million customers, or one in six Kenyans. Operators in several emerging countries have followed, and by end-2009 CGAP expects more than 120 mobile money implementations in developing markets.

HEALTH IT

Doctor builds Web care system

Clinics to feature e-mail, videochats with providers

BY LISA WANGSNES, *THE BOSTON GLOBE*

NEW YORK - Dr. Jay Parkinson favors black jeans. He has a blog where he posts thoughts such as "I can't wait to make a car honk using only my iPhone."

Sitting before a laptop in a loft-style office in Brooklyn's Williamsburg neighborhood, he talks about what ails the US healthcare system - skyrocketing costs, excessive use, bureaucracy - and why the cure is not the universal insurance Democrats are talking about on Capitol Hill, but rather "disruptive technology."

He means technology that jolts systems into making dramatic progress or the Facebook-style software he is developing for Hello Health, a national franchise of clinics he is building where patients can e-mail, text, or videochat with doctors over a secure website.

"We have in-person relationships with patients in our neighborhood, and we communicate the way we all communicate nowadays," he says.

Fast Company magazine has hailed the 33-year-old Parkinson as "The Doctor of the Future" because he aims to bring to medicine the kind of easy relationship to technology that most doctors have not yet embraced.

An ad for the company promises: "No more frantic Googling, no more whole days away from work, no more long waits, and no more unnecessary ER visits, or scary receptionists."

The simplicity and visual appeal of demonstrations of the Hello Health software platform have made him a celebrity in the health technology world.

Whether Hello Health will be able to live up to the hype remains in question. The three-physician demonstration clinic he opened last July has treated 700 patients, 400 of whom have become regular patients. The average primary care office has perhaps 2,500 patients per doctor; the average concierge practice has 800 to 1,000.

The company plans to add clinics in New York and elsewhere this summer.

And Parkinson, who was trained as a pediatrician but no longer practices because he is working full time on developing the company, and Nat Findlay, the firm's Canadian

cofounder, are both optimistic about their chances.

The Hello Health website, to be launched this summer, will give patients access to a secure website where they can exchange messages with their doctor in a blog-style format. Specialists could eventually join the conversation (imagine your family doctor meeting with your neurologist, and you get a written record of what everyone said.)

In an early version, patients can pay bills, schedule appointments, or view medical records and lab results in a couple of clicks.

At the Williamsburg practice, a quick visit with a doctor, in person or online, costs \$100; more complex visits cost \$200. Simple e-mailed questions are covered under the \$35 per month membership fee. Hello Health does not accept insurance, though patients who are insured can send the bills to their insurance company for reimbursement.

Most insurers will not pay doctors for answering simple questions from patients by e-mail; reimbursement usually depends on an in-person office visit. Less than 20 percent of doctors e-mail their patients, and even fewer talk with them on Skype, said Steven Waldren, director of the Center for Health Information Technology of the American Academy of Family Physicians.

"Right now, in most of the current insurance plans, all I can do is see you in the office. . . . That's the only way to get reimbursed," Waldren said.

Medicare and some insurance companies have begun to provide incentives for using technology to improving quality, he said, but it is not anywhere near the same money as an office visit.

Hello Health has invented "a financial model that allows them to step outside those constraints and experiment and innovate," Waldren said.

Hello Health is targeting the small group of patients in the \$2.5 trillion-a-year US healthcare industry who pay most of their bills in cash or by credit card, mostly those without insurance or with high-deductible plans. But Congress, as part of a massive health overhaul, is strongly considering a mandate that everyone have insurance.

Parkinson says it doesn't matter. The national shortage of primary care doctors is getting worse, because doctors are not paid enough and have too little time with patients.

More at http://www.boston.com/news/nation/articles/2009/06/21/hello_health_clinics_would_offer_medical_care_online/?page=2

HEALTH IT - II

Group advocates electronic medical records

HealthDataRights.org wants patients to have better access to their own information.

BY W.J. HENNIGAN, *LOS ANGELES TIMES*

Accessing your own medical records should be as easy as checking your online bank account, a new health-data group contends, and Monday it launched a website to promote better access.

The site, HealthDataRights.org, was established by a group that is boosting greater personal use of electronic medical records. Only 15% of physicians track the records electronically, said James Heywood, a group founder.

"We want to move toward a world in which patients have complete access to their medical information," he said. "Patients have the right to help themselves."

Administration urged to engage public on e-health records

BY ALIYA STERNSTEIN, *NEXTGOV*

As the Obama administration seeks to determine who uses electronic health records and for what purposes, some health information technology specialists say it is critical that the public provide feedback on the issue. They note it could dictate how billions of economic stimulus dollars are spent.

The 2009 American Recovery and Reinvestment Act allocated about \$20 billion to encourage doctors and hospitals to install e-records systems by 2014. Medical professionals who make "meaningful use" of e-records by 2011 or 2012 would be eligible for up to \$44,000 in Medicare payments spread out over five years. An advisory committee within the Health and Human Services Department met on June 16 to begin defining meaningful use.

While HHS opened the meeting to the public and is seeking comment on proposed recommendations, "they could go further to talk about a variety of different public and consumer uses and sort of their vision for where they want this [process] to go," said Michael W. Painter, senior program officer at the Robert Wood Johnson Foundation, a philanthropic organization that focuses on health issues. For example, a Google consumer health application could meet the meaningful standard and should be discussed in public forums, he said.

"I thought the meeting was excellent and thought-provoking . . . [but] the vision they come up with and the definitions they create should incorporate a specific role for the public," Painter said.

Heywood is chairman and co-founder of Patients Like Me, a social networking health site. He said a major roadblock in many states are laws that make it cumbersome for doctors to turn over information to patients.

Almost \$60 billion in the 2009 federal economic stimulus package has been designated for healthcare, including a sizable chunk to help the electronic transition.

The transition is the linchpin for the website's cause. In digital form, the information is easier to store, update and exchange. The next step is getting patients access, Heywood said.

Some privacy advocates are wary of how electronic medical records will be used. Lee Tien, a senior attorney at the Electronic Frontier Foundation in San Francisco, agrees that patients should have more access to their records, but not at the expense of security.

Source: <http://www.latimes.com/business/la-fi-medical-records23-2009jun23,0,3099873.story>

One predicament might be that federal officials and the public are talking past each other: Americans are weighing in on health care reform via opinion polls, and White House officials have said they want feedback on administration proposals, but the two sides do not have a forum for direct communication, say some health care system critics.

"In my view, there are parallel universes of health care reform discussion. One is what everyday people are saying and thinking. . . . And, yes, the White House hopes people will visit its site on reform and weigh in," said Brian Klepper, managing principal of Florida-based market research firm Healthcare Performance Inc. "The core problem here is that there is no political power center for regular people toglom on to health care reform."

Furthermore, some potential meaningful uses will be more important to patients than providers, insurers, vendors and everyone else getting health IT stimulus funding. Some observers argue that the definition of meaningful use should explicitly grant patients the right to access data entered by physicians or even own it so they can take it and pursue treatment elsewhere.

In testimony on May 20 before an HHS advisory panel, Marc Donner, director of engineering for Google Health, said, "Requiring recipients of federal funds who purchase EHRs to make patient medical records available online in [compatible formats], using nonproprietary vocabularies where possible, would further encourage [information sharing] and portability, both of which are key components to increased consumer adoption and empowerment."

More at http://www.nextgov.com/nextgov/ng_20090623_2200.php

PRIVACY AND SECURITY

Government surveillance response 'inadequate', say Lords

The Government's response to a Parliamentary report on the monitoring and legislation surrounding surveillance is "inadequate" and it has "paid insufficient attention" to the report's recommendations, a follow up report has said.

OUT-LAW NEWS

The House of Lords Select Committee on the Constitution produced a report earlier this year which made a series of recommendations on how the law and Government behaviour should change in order to protect citizens and their privacy as data gathering and surveillance becomes more pervasive.

The report said that there should be judicial oversight of surveillance, and that the increasing monitoring of citizens was breaking the bond of trust between the Government and the people.

The Government rejected most of the report's recommendations and claimed that its current and planned policies give an effective balance between personal privacy and state security.

The House of Lords Committee has hit back, saying that the Government's response fails to understand or address the scale of the problem.

"We regret that the Government have not agreed to a number of important recommendations which sought to assist the executive in promoting the responsible and proper use of data processing, including data sharing, together with other modes of surveillance," its response said. "The Government have paid insufficient attention to a number of fundamental points and criticisms made in the Report."

The Lords' analysis of the Government response accused it of seeming to agree with the Lords without outlining any effective action.

"The response reiterates the need to balance privacy with security and other objectives, and to ensure that the principles of necessity and proportionality are adhered to, without sufficiently indicating how this can be achieved," it said.

Much of the Government's response rested on its recommendation that Government departments use privacy impact assessments (PIA) to ensure that policies do not harm people's privacy. The Lords' analysis was scathing about how much good such reports could do.

More at <http://www.out-law.com//default.aspx?page=10112>

Social networking giants are subject to EU data protection laws, say regulators

Social networking sites are legally responsible for their users' privacy, Europe's privacy watchdogs have confirmed. A committee of data protection regulators has said that the sites are 'data controllers', with all the legal obligations that brings.

OUT-LAW NEWS

Users of the sites are also data controllers with legal obligations when they are posting on behalf of a club, society or company, the opinion said.

The committee of Europe's data protection regulators, the Article 29 Working Party, has published its opinion on the legal status of social networking operators such as Facebook and MySpace.

It has said that the sites cannot escape their legal obliga-

tions just because content on them is often produced and posted by users.

"SNS [Social Network Service] providers are data controllers under the Data Protection Directive," it said. "They provide the means for the processing of user data and provide all the 'basic' services related to user management (e.g. registration and deletion of accounts). SNS providers also determine the use that may be made of user data for advertising and marketing purposes – including advertising provided by third parties."

Being a data controller under data protection legislation brings with it greater legal responsibilities than being a data processor: The opinion said that social networking companies count as data controllers under EU law "even when their headquarters are outside of the [European Economic Area]".

The opinion said that users of social networking sites could also attract the same legal obligations, but only if they were acting on behalf of a company, association or in pursuit of commercial, political or charitable goals.

The opinion also outlines the obligations of people who count as data processors.

More at <http://www.out-law.com//default.aspx?page=10113>

PRIVACY AND SECURITY - II

Prescription drug fight goes before appeals court

BY LARRY NEUMEISTER, *THE ASSOCIATED PRESS*

NEW YORK - So-called data-mining companies that collect information about the drugs doctors prescribe asked an appeals court Tuesday to stop Vermont from enacting a law next week restricting their work.

Attorney Thomas Julin told a three-judge panel of the 2nd U.S. Circuit Court of Appeals that it would violate the First Amendment rights of the companies if the law is enacted on July 1.

He asked the appeals court to block implementation of the law until it decides whether to uphold a lower court ruling that concluded the law did not violate the Constitution. Both sides were expected to submit written arguments in the wider appeal case within two months.

The court did not immediately rule, but Judge Barrington Parker called it a fascinating case.

Julin, representing IMS Health Inc., Verispan LLC and Source Healthcare Analytics Inc., told the judges that information gathered by the companies is noncommercial speech protected by the First Amendment. He said the companies are the world's leading publishers of information regarding the pharmaceutical and health care industries.

The companies gather electronic information on drugs ordered by doctors for their patients and sell that information to pharmaceutical companies. In court papers, they said they also publish unique reports - "a form of specialized news reporting" - showing which doctors prescribe which medications most frequently.

In separate courts, the companies have tried to block laws restricting their activities in New Hampshire, Maine and Vermont. More than 20 state legislatures have looked at the issue, advocates on both sides say.

Bridget Asay, an assistant attorney general, urged the appeals judges to let the law take effect, saying no substantial First Amendment issues were at stake. She called the work done by the companies a "covert marketing tool."

In court papers, she said blocking the law's enforcement was a drastic measure not necessary after a court fight that has already stretched 20 months.

She said Vermont's Prescription Confidentiality Law regulates commercial marketing of certain health care records to promote public health, medical privacy and to contain health care costs.

More at <http://www.washingtonpost.com/wp-dyn/content/article/2009/06/23/AR2009062303254.html>

DOD creates Cyber Command as U.S. Strategic Command subunit *New post will defend .mil domain*

BY WILLIAM JACKSON,

FEDERAL COMPUTER WEEK

Defense Secretary Robert Gates issued a much-anticipated order June 23 establishing the U.S. Cyber Command, which will assume responsibility for the defense of the military's portion of cyberspace.

The new Cybercom will be a subunit of the U.S. Strategic Command and will be commanded by the director of the National Security Agency. It is expected to be headquartered with NSA at Fort Meade, Md., and to reach initial operating capacity in October, with full operating capacity coming in October 2010.

The order is recognition that cyberspace is a distinct military domain, along with land, sea and air, and the Defense Department must be prepared to defend and conduct offensive operations in it.

"Cyberspace and its associated technologies offer unprecedented opportunities to the United States and are vital to our nation's security and, by extension, to all aspects of military operations," Gates wrote in his order. "Yet our increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to our national security. To address this risk effectively and to secure freedom of action in cyberspace, the Department of Defense requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations."

Planning for Cybercom has been in the works for some time, and the order has been expected for several weeks. Observers in the cybersecurity field have said such coordination of defensive and offensive activities is needed to ensure the security and availability of the critical information infrastructure.

Alan Paller, director of research at the SANS Institute, called the command a "spectacular idea" because it allows defense to be informed by offensive capabilities and offers the potential for increased interoperability, information sharing and visibility.

More at <http://fcw.com/articles/2009/06/24/dod-launches-cyber-command.aspx>

NEW REPORTS AND PAPERS

Some Patients Are Not Notified of Abnormal Test Results

AMERICAN MEDICAL ASSOCIATION

Newswise — Primary care clinicians and their staff appear to fail to inform some patients, or to fail to document informing patients, about abnormal results on outpatient medical tests, according to a report in the June 22 issue of *Archives of Internal Medicine*, one of the JAMA/Archives journals.

“Ordering and following up on outpatient laboratory and imaging tests consumes large amounts of physician time and is important in the diagnostic process,” the authors write as background information in the article. “Diagnostic errors are the most frequent cause of malpractice claims in the United States; testing-related mistakes can lead to serious diagnostic errors. There are many steps in the testing process, which extends from ordering a test to providing appropriate follow-up; an error in any one of these steps can have lethal consequences.”

Lawrence P. Casalino, M.D., Ph.D., of Weill Cornell Medical College, New York, and colleagues reviewed the medical records of 5,434 randomly selected patients age 50 to 69 years in 23 primary care practices (19 community-based and four affiliated with academic medical centers). The researchers identified individuals with a clinically significant abnormal result on one of 11 blood tests or three screening tests commonly performed on an outpatient basis. These patients' records were then assessed for an indication that he or she had been informed about the abnormal result. In cases for which there was no evidence such communication occurred, physicians were sent a form alerting them to the apparent oversight and giving them the opportunity to correct the record if the patient had been informed or to inform the patient at that time.

In addition, physicians responded to a six-question survey

about the processes for managing test results at their practices and their satisfaction with these processes. Reviewers calculated a score ranging from zero to five for each practice, with five indicating that they closely followed five processes derived from the medical literature—routing results to the responsible physician, having the physician sign off on the results, informing the patient of all results (normal and abnormal, at least in general terms) and asking patients to call after a certain time period if they had not been notified of the results.

The reviewers identified 1,889 abnormal test results and 135 apparent failures to inform the patient or to document informing the patient—a rate of 7.1 percent, or about one of every 14 tests. The average process score was 3.8; most practices did not use all five of the basic processes suggested in the literature and most did not have explicit rules for notifying patients of results. “Failure rates varied widely among practices, from 0 percent to 26 percent; practices that used better processes to manage results had lower failure rates and had physicians who were more satisfied with the processes used,” the authors write.

Practices that used a combination of paper and electronic records—a so-called partial electronic medical record—had the highest failure rates, whereas there was no significant difference between practices that used complete electronic medical records or paper records.

“Some elements of medical care (e.g., diagnosis) are an art as well as a science, depend heavily on the cognitive skills and effort of individual physicians, involve much uncertainty and will probably always have relatively high error rates,” the authors conclude. “However, notifying patients of test results does not appear to be such a process; with appropriate within-practice systems, low rates of failure to inform should be possible.”

Source: <http://www.newswise.com/articles/view/553557/>

CDT Releases Report Tracking Cyberspace Policy Review Privacy Action Items

CENTER FOR DEMOCRACY AND TECHNOLOGY

CDT today released a report to help track the progress of the privacy "action items" contained in the Administration's recently released Cyberspace Policy Review. The Review discusses a

wide range of issues that the country needs to address in order to ensure that national security, economic and civil liberties interests are adequately protected. The action items outlined in the CDT report were derived from the Review and President's subsequent remarks on the document. The action items that develop from these themes are offered to supplement the Review's broader near and mid-term Action Plan for the incoming Cybersecurity Policy Official.

More at <http://www.cdt.org/headlines/1224>

NEW REPORTS AND PAPERS - II

Opinion 5/2009 on online social networking

DATA PROTECTION WORKING PARTY

Executive Summary

This Opinion focuses on how the operation of social networking sites can meet the requirements of EU data protection legislation. It principally is intended to provide guidance to SNS providers on the measures that need to be in place to ensure compliance with EU law. The Opinion notes that SNS providers and, in many cases, third party application providers, are data controllers with corresponding responsibilities towards SNS users. The Opinion outlines how many users operate within a purely personal sphere, contacting people as part of the management of their personal, family or household affairs. In such cases, the Opinion deems that the 'household exemption' applies and the regulations governing data controllers do not apply. The Opinion also specifies circumstances whereby the activities of a user of an SNS are not covered by the 'household exemption'. The dissemination and use of information available on SNS for other secondary, unintended purposes is of key

concern to the Article 29 Working Party. Robust security and privacy-friendly default settings are advocated throughout the Opinion as the ideal starting point with regard to all services on offer. Access to profile information emerges as a key area of concern. Topics such as the processing of sensitive data and images, advertising and direct marketing on SNS and data retention issues are also addressed.

Key recommendations focus on the obligations of SNS providers to conform with the Data Protection Directive and to uphold and strengthen the rights of users. Of paramount importance, SNS providers should inform users of their identity from the outset and outline all the different purposes for which they process personal data. Particular care should be taken by SNS providers with regard to the processing of the personal data of minors. The Opinion recommends that users should only upload pictures or information about other individuals, with the individual's consent and considers that SNS also have a duty to advise users regarding the privacy rights of others.

More at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf

Content and Frequency of Writing on Diabetes Bulletin Boards: Does Race Make a Difference?

BY SIOBHAN CASE, BA; VALARIE JERNIGAN, DRPH; AUDRA GARDNER, PHD; PHILIP RITTER, PHD; CATHERINE A HEANEY, PHD; KATE R LORIG, RN, DRPH, *STANFORD UNIVERSITY*

ABSTRACT

Background: Diabetes-related disparities are well documented among racial minority groups in the United States. Online programs hold great potential for reducing these disparities. However, little is known about how people of different races utilize and communicate in such groups. This type of research is necessary to ensure that online programs respond to the needs of diverse populations.

Objective: This exploratory study investigated message frequency and content on bulletin boards by race in the Internet Diabetes Self-Management Program (IDSMP). Two questions were asked: (1) Do participants of different races utilize bulletin boards with different frequency? (2) Do message, content, and communication style differ by race? If so, how?

Methods: Subjects were drawn by purposeful sampling from participants in an ongoing study of the effectiveness of the

IDSMP. All subjects had completed a 6-week intervention that included the opportunity to use four diabetes-specific bulletin boards. The sample (N = 45) consisted of three groups of 15 participants, each who self-identified as American Indian or Alaskan Native (AI/AN), African American (AA), or Caucasian, and was stratified by gender, age, and education. Utilization was assessed by counting the number of messages per participant and the range of days of participation. Messages were coded blindly for message type, content, and communication style. Data were analyzed using descriptive and nonparametric statistics.

Results: In assessing board utilization, AAs wrote fewer overall messages (P = .02) and AIs/ANs wrote fewer action planning posts (P = .05) compared with Caucasians. AIs/ANs logged in to the program for a shorter time period than Caucasians (P = .04). For message content, there were no statistical (P ≤ .05) differences among groups in message type. No differences were found in message content between AAs and Caucasians, but AIs/ANs differed in content from both other groups. Caucasians wrote more on food behaviors than AIs/ANs (P = .01), and AIs/ANs wrote more about physical activity than Caucasians (P = .05) and about walking than the other two groups (P = .01). There were no differences in communication style.

Conclusions: Although Caucasians utilized the boards more than the other two groups, there were few differences in message type, content, or style.

More at <http://www.jmir.org/2009/2/e22/>

NEW REPORTS AND PAPERS - III

Frequency of Failure to Inform Patients of Clinically Significant Outpatient Test Results

BY LAWRENCE P. CASALINO, MD, PHD; DANIEL DUNHAM, MD, MPH; MARSHALL H. CHIN, MD, MPH; REBECCA BIELANG, MD; EMILY O. KISTNER, PHD; THEODORE G. KARRISON, PHD; MICHAEL K. ONG, MD, PHD; URMIMALA SARKAR, MD, MPH; MARGARET A. MCLAUGHLIN, MD; DAVID O. MELTZER, MD, PHD, *ARCHIVES OF INTERNAL MEDICINE*

ABSTRACT

Background: Failing to inform a patient of an abnormal outpatient test result can be a serious error, but little is known about the frequency of such errors or the processes for managing results that may reduce errors.

Methods: We conducted a retrospective medical record review of 5434 randomly selected patients aged 50 to 69 years in 19 community-based and 4 academic medical center primary care practices. Primary care practice physicians were surveyed about their processes for managing test results, and individual physicians were notified of apparent failures to inform and asked whether they had informed the patient. Blinded reviewers calculated a "process score" ranging from 0 to 5 for each practice using survey responses.

Results: The rate of apparent failures to inform or to docu-

ment informing the patient was 7.1% (135 failures divided by 1889 abnormal results), with a range of 0% to 26.2%. The mean process score was 3.8 (range, 0.9-5.0). In mixed-effects logistic regression, higher process scores were associated with lower failure rates (odds ratio, 0.68; $P < .001$). Use of a "partial electronic medical record" (paper-based progress notes and electronic test results or vice versa) was associated with higher failure rates compared with not having an electronic medical record (odds ratio, 1.92; $P = .03$) or with having an electronic medical record that included both progress notes and test results (odds ratio, 2.37; $P = .007$).

Conclusions: Failures to inform patients or to document informing patients of abnormal outpatient test results are common; use of simple processes for managing results is associated with lower failure rates.

INTRODUCTION

Ordering and following up on outpatient laboratory and imaging tests consumes large amounts of physician time and is important in the diagnostic process.¹⁻² Diagnostic errors are the most frequent cause of malpractice claims in the United States³⁻⁴; testing-related mistakes can lead to serious diagnostic errors.⁵ There are many steps in the testing process, which extends from ordering a test to providing appropriate follow-up⁶; an error in any one of these steps can have lethal consequences.^{3, 7-8} In this article, we focus on one step in the process: informing the patient of test results. Failures to inform patients of abnormal results and failures to document that patients have been informed are common and legally indefensible factors in malpractice claims.^{7, 9}

More at <http://archinte.ama-assn.org/cgi/content/full/169/12/1123>

Coping With Digital Revolution: China Offers Green Dam, Iran Faces Neda

Despite many counter-measures and filters, digital democracy continues to trouble authoritarian regimes

BY GUOBIN YANG, *YALE GLOBAL*

NEW YORK: Recent events in Iran and China have again demonstrated the global power of the Internet. Iranians used web technologies to broadcast their street protests to the world while Chinese netizens challenged a government policy to require computers to pre-install a new filtering software.

In Iran, protesters used the social-networking tool Twitter to communicate with the outside world when journalists' access

was restricted. Large numbers of tweeters individually reported the events with photographs, short messages, and links to videos and web sites. The result was a real-time communication network that beamed out information about the current Iranian crisis almost non-stop. This is the power of a new type of CNN – a Citizen News Network.

In China, the announcement of a government policy to require computers to pre-install a software called "Green Dam-Youth Escort" triggered a backlash of online protest. The policy was allegedly designed to protect minors from pornography and other "unhealthy contents" online. Although few would object to protecting minors and China undoubtedly has its share of trouble in battling Internet pornography, the new policy raises serious questions about its hidden intentions.

More at <http://yaleglobal.yale.edu/display.article?id=12493>

NEW REPORTS AND PAPERS - IV

Facebook, Youtube+: How Social Media Outlets Impact Digital Terrorism And Hate

SIMON WIESENTHAL CENTER

The recent arrests in the tragic murders of Stephen Tyrone Jones at the U.S. Holocaust Museum and Dr. George Tiller at his Kansas church uncovered more evidence of how viral hate online incubates, empowers and emboldens violent bigots. With over one and a half billion users (almost one quarter of the world's population), the Internet is the prime means of communication and marketing in the world. The Internet's unprecedented global reach and scope combined with the difficulty in monitoring and tracing communications make it the prime tool for extremists and terrorists. The Simon Wiesenthal Center has been monitoring these developments for over a decade through its Digital Terrorism and Hate Project.

At a press briefing on Thursday June 18, at 11:00 a.m., the Wiesenthal Center will present Facebook, YouTube +: How Social Media Outlets Impact Digital Terrorism and Hate, a report that confirms again that as the Internet has grown, the escalation of extremist sites has kept pace in number and in technological sophistication especially with developments in dynamic new social networking services. Sites such as Facebook and YouTube have both seen a huge proliferation of extremist use with the greatest increase coming from overseas, particularly Europe and the Middle East. The CD-ROM report, released annually, is designed to assist law enforcement, public officials, educators, parents and the news media to better grasp the scope of hate. The report is used by the FBI, Homeland Security, military officials, hate crime units and joint terrorism taskforces in the U.S. as well as Canada and Europe.

More at <http://www.wiesenthal.com/site/apps/nlnet/content2.aspx?c=lsKWLbPJLnF&b=4441467&ct=7131713>

Peeping

BY PETER P. SWIRE, *MORITZ COLLEGE OF LAW OF OHIO STATE UNIVERSITY*

Abstract:

This article explores the phenomenon of employee snooping, which I call "peeping." The essay draws on mythology and literature to show the ancient roots of the phenomenon of peeping, and hopefully encourages discussion and raises awareness of peeping throughout the academic community.

Part I of the essay discusses recent political and celebrity peeping incidents, such as the passport records of candidate Obama.

Part II describes three, increasingly harmful, types of peeping; "the gaze," "the gossip," and "the grab." The "gaze" occurs simply when a person looks at another person without permission, such as Peeping Tom gazing at Lady Godiva or a modern-day Peeping Tom sneaking a peek into a database. The "gossip" occurs when the person tells other what he or she has seen. The "grab" is even more serious. It occurs when an employee grabs the personal information for profit, often at the behest of an outsider. A recent example is where the National Enquirer paid an employee at the UCLA Medical Center to turn over celebrities' medical records on over 30 occasions.

Part III asks: "Why now?" Human curiosity, especially for the titillating or about the famous, is as old as human nature. There are specific reasons, however, why these peeping

incidents are coming to our attention now. The number of detailed databases, accessible by numerous employees, has climbed sharply in recent years. Once a peeping incident occurs, the perpetrator can easily post the evidence to a blog or social networking site. Such databases also increasingly have logging and auditing software, so that the peepers can be caught after the fact. In short, the opportunity for peeping has climbed, and the possibility of catching the peeper has climbed as well. As a society, therefore, we are newly facing the question of how to respond when we catch the perpetrators.

Part IV explores what to do about this increase of peeping. The penalty for peeping for Tiresias and Tom was blindness, but that seems a bit excessive. Many of the most promising approaches are technical safeguards, and there are also useful administrative safeguards, from training employees to considering expanding the new California law giving notice in the event of a peep.

Part V applies these insights to a major current area of controversy - behavioral advertising on the Internet. A significant source of concern about tracking the Internet usage of individuals is that they will become subject to peeping, as happened for instance to Obama's cell phone records once he became famous.

In short, this essay can encourage more discussion about peeping for writers from many fields beyond law and technology, including literature, mythology, sociology, anthropology, psychology and more besides.

More at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1418091

NEW REPORTS AND PAPERS - V

Author Autonomy and Atomism in Copyright Law

BY MOLLY SHAFFER VAN HOUWELING,
UNIVERSITY OF CALIFORNIA

Abstract:

The power and ubiquity of personal computing and the Internet have enabled individuals - even impecunious amateurs - to create and communicate in ways that were previously possible only for well-funded corporate publishers. These individual creators are increasingly harnessing copyright law - insisting on ownership of their rights and controlling the ways in which those rights are licensed to others. Facebook users are demanding ownership of their online musings. Scholars are archiving their research online and refusing to assign their copyrights to publishers. Independent musicians are streaming their own songs and operating without record companies. Organizations like the Free Software Foundation are encouraging individual authors to manage their copyrights in innovative ways.

When the myriad individual authors empowered by today's ubiquitous digital technology claim, retain, and manage their own copyrights, they exercise a degree of authorial autonomy that befits the Internet Age. But they simultaneously contribute to a troubling phenomenon I call "copyright atomism" - the proliferation, distribution, and fragmentation of the exclusive rights bestowed by copyright law, and of idiosyncratic permutations of those rights. The information and transaction costs associated with atomism could hamper future generations of technology-fueled creativity and thus undermine the very purpose of copyright: to encourage the creation and dissemination of works of authorship for the ultimate benefit of the public.

In this project I aim to place contemporary copyright atomism in historical and doctrinal context by documenting copyright law's previous encounters with proliferated, distributed, and fragmented copyright ownership. Along the way I examine how copyright law has encouraged and discouraged atomism and managed its consequences.

More at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1422016

I'm Losing Patience with Your Site: The Impact of Information Scent and Time Constraints on Effort, Performance, and Attitudes

Proceedings of the International Conference on Information Systems, December 14, 2008

BY GREG MOODY AND DENNIS GALLETTA,
UNIVERSITY OF PITTSBURGH

Abstract:

As competition increases in the online world, website

owners will investigate ways in which they can attract more users. Additionally, many consumers suffer ever-increasing time limitations when browsing for a particular item on a website. Users can become frustrated and stressed when they are unable to find those items due to poor information scent, or semantic cues that are meant to lead to their goal. This paper presents and tests a theoretical model to predict how information scent can reduce the amount of stress that consumers experience when seeking information under time constraints. The study also demonstrates the relationships between information scent, time constraints, stress, performance and attitudes toward the website. Results indicate that while high information scent is an important design goal, scent can only be assessed by taking the user's task into account.

Source: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1420990

How Open is Open Enough? Melding Proprietary and Open Source Platform Strategies

BY JOEL WEST, *SAN JOSE STATE UNIVERSITY*

Abstract:

Computer platforms provide an integrated architecture of hardware and software standards as a basis for developing complementary assets. The most successful platforms were owned by proprietary sponsors that controlled plat-

form evolution and appropriated associated rewards.

Responding to the Internet and open source systems, three traditional vendors of proprietary platforms experimented with hybrid strategies which attempted to combine the advantages of open source software while retaining control and differentiation. Such hybrid standards strategies reflect the competing imperatives for adoption and appropriability, and suggest the conditions under which such strategies may be preferable to either the purely open or purely proprietary alternatives.

Source: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=894363#

POINTS OF VIEW

Cyber-Scare

The exaggerated fears over digital warfare

BY EVGENY MOROZOV, *BOSTON REVIEW*

The age of cyber-warfare has arrived. That, at any rate, is the message we are now hearing from a broad range of journalists, policy analysts, and government officials. Introducing a comprehensive White House report on cyber-security released at the end of May, President Obama called cyber-security “one of the most serious economic and national security challenges we face as a nation.” His words echo a flurry of gloomy think-tank reports. The Defense Science Board, a federal advisory group, recently warned that “cyber-warfare is here to stay,” and that it will “encompass not only military attacks but also civilian commercial systems.” And “Securing Cyberspace for the 44th President,” prepared by the Center for Strategic and International Studies, suggests that cyber-security is as great a concern as “weapons of mass destruction or global jihad.”

Unfortunately, these reports are usually richer in vivid metaphor—with fears of “digital Pearl Harbors” and “cyber-Katrinass”—than in factual foundation.

Consider a frequently quoted CIA claim about using the Internet to cause widespread power outages. It derives from a public presentation by a senior CIA cyber-security analyst in early 2008. Here is what he said:

We have information, from multiple regions outside the United States, of cyber-intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyber-attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet.

So “there is information” that cyber-attacks “have been used.” When? Why? By whom? And have the attacks caused any power outages? The CIA may have some classified information, but very little that is unclassified suggests that such cyber-intrusions have occurred.

Or consider an April 2009 Wall Street Journal article entitled “Electricity Grid in U.S. Penetrated By Spies.” The article quotes no attributable sources for its starkest claims about cyber-spying, names no utility companies as victims of intrusions, and mentions just one real cyber-attack, which occurred in Australia in 2000 and was conducted by a disgruntled employee rather than an external hacker.

It is alarming that so many people have accepted the White

House’s assertions about cyber-security as a key national security problem without demanding further evidence. Have we learned nothing from the WMD debacle? The administration’s claims could lead to policies with serious, long-term, troubling consequences for network openness and personal privacy.

Cyber-security fears have had, it should be said, one unambiguous effect: they have fueled a growing cyber-security market, which, according to some projections, will grow twice as fast as the rest of the IT industry. Boeing, Raytheon, and Lockheed Martin, among others, have formed new business units to tap increased spending to protect U.S. government computers from cyber-attacks. Moreover, many former government officials have made smooth transitions from national cyber-security policy to the lucrative worlds of consulting and punditry. Speaking at a recent conference in Washington, D.C., Amit Yoran—a former cyber-security czar in the Bush administration and currently the C.E.O. of NetWitness, a cyber-security start-up—has called hacking a national security threat, adding that “cyber-9/11 has happened over the last ten years, but it’s happened slowly, so we don’t see it.” One way for the government to protect itself from this cyber-9/11 may be to purchase NetWitness’s numerous software applications, aimed at addressing both “state and non-state sponsored cyber threats.”

From a national security perspective, cyber-attacks matter in two ways. First, because the back-end infrastructure underlying our economy (national and global) is now digitized, it is subject to new risks. Fifty years ago it would have been hard—perhaps impossible, short of nuclear attack—to destroy a significant chunk of the U.S. economy in a matter of seconds; today all it takes is figuring out a way to briefly disable the computer systems that run Visa, MasterCard, and American Express. Fortunately, such massive disruption is unlikely to happen anytime soon. Of course there is already plenty of petty cyber-crime, some of it involving stolen credit card numbers. Much of it, however, is due to low cyber-security awareness by end-users (you and me), rather than banks or credit card companies.

Second, a great deal of internal government communication flows across computer networks, and hostile and not-so-hostile parties are understandably interested in what is being said. Moreover, data that are just sitting on one’s computer are fair game, too, as long as the computer has a network connection or a USB port. Despite the “cyber” prefix, however, the basic risks are strikingly similar to those of the analog age. Espionage has been around for centuries, and there is very little we can do to protect ourselves beyond using stronger encryption techniques and exercising more caution in our choices of passwords and Wi-Fi connections.

To be sure, there is a war-related caveat here: if the military relies on its own email system or other internal electronic communications, it is essential to preserve this capability in wartime.

More at <http://bostonreview.net/BR34.4/morozov.php>

POINTS OF VIEW - II

How to Cut Health-Care Costs: Less Care, More Data

BY MICHAEL GRUNWALD, *TIME*

Ezekiel Emanuel got a memorable introduction to our haphazard health-care system on his first visit to a cancer ward as a medical student. The white coats were ordering a transfusion for a teenage girl, and since shyness does not run in his family — brother Rahm is President Obama's famously foulmouthed chief of staff, brother Ari a similarly silence-deficient Hollywood agent — he interrupted to ask why. Because she had Hodgkin's disease and her platelets were below 20,000, the team explained. Emanuel still had questions: Was there evidence for that protocol? Don't some hospitals wait until 10,000? Why 20,000? Because that's what we do here, one doc replied.

Now a noted oncologist turned White House health adviser, Emanuel has spent much of his career battling the that's-what-we-do-here mentality of American medicine. "It drives me nuts — the ignorance is overwhelming," he says. "I'm a data-driven guy. I want to see evidence." It turns out that Emanuel's boss, budget director Peter Orszag, is also a data-driven guy, as is Orszag's boss, the President of the United States. They've already stuffed \$1.1 billion into the stimulus bill to jump-start "comparative effectiveness research" into which treatments work best in which situations. Now they're pushing to overhaul the entire health-care sector by year's end, and they're determined to replace ignorance with evidence, to create a data-driven system, to shift one-sixth of the economy from "that's what we do here" to "that's what works." (Watch a video about a woman living without health insurance.)

The U.S. spends more on health care than any other country does, and studies have suggested that as much as 30% of it — perhaps \$700 billion a year — may be wasted on unneeded care, mostly routine CT scans and MRIs, office visits, hospital stays, minor procedures and brand-name prescriptions that are requested by patients and ordered by doctors every day. Orszag is particularly obsessed with research by the Dartmouth Institute for Health Policy and Clinical Practice, documenting huge regional variations in costs but virtually no variations in outcomes. For example, chronically ill patients in Los Angeles visited doctors an average of 59.2 times in the last six months of their life, vs. only 14.5 times in Ogden, Utah; they still ended up just as dead. Medicare now pays three times as much per enrollee in Miami as in Honolulu, and costs are growing twice as fast in Dallas as in San Diego. Patients in higher-spending regions get more tests, more procedures, more referrals to specialists and more time in the hospital and ICU, but the Dartmouth research has found that if anything, their outcomes are slightly worse. "We're flying blind," says Dartmouth's Dr. Elliott Fisher. "We're getting quantity, not quality."

Why Less Would Be More

Americans tend to assume that more is better, especially when it comes to the heroic brand of try-everything medicine we've watched on ER and House M.D. But overtreatment is a national scandal. It's bad for our health: with medical errors now estimated to be our eighth leading cause of death, drugs, procedures and hospital stays can be risky (as well as painful, time-consuming and wallet-straining) even when they're necessary. It's also bad for the economy: health costs are bankrupting small businesses and even conglomerates like General Motors as well as millions of families. And it's awful for the country: Medicare is on track to go broke by 2017, and our long-term budget problems are primarily health-cost problems. At current growth rates, health spending by the Federal Government alone would increase from 5% to 20% of the economy by 2050; Social Security, by contrast, would increase only from 5% to 6%.

Alas, there's no proven link between more spending and better care. The good news is that parts of the country provide care at a low cost, so there's potential for gigantic savings if the rest of the U.S. could imitate them. One Dartmouth study found that if nationwide spending had mirrored the modest rate of that in Rochester, Minn. — where care is dominated by the renowned Mayo Clinic — Medicare would have reduced its costs for chronically ill patients by \$50 billion from 2001 to 2005. As the old inflation-adjusted saying goes, pretty soon you're talking about real money.

But one man's unnecessary costs are another man's profits; lobbyists for drug- and devicemakers, hospitals, doctors and insurers are already fighting to make sure their slices of the more than \$2 trillion health-care pie aren't nibbled by reform. Senate Republicans just introduced "antirationing" legislation to bar the government from using comparative-effectiveness research — "a common tool used by socialized health-care systems" — for cost control. They paused in their usual attacks on Obama's profligacy just long enough to attack his stinginess, warning that he will use evidence as an excuse to micromanage the art of medicine, stifle innovation and deny Americans their right to choose whatever treatments they want — or at least their right to taxpayer reimbursements.

Some of this is transparent posturing, but there are legitimate concerns about politicians' deciding when treatments are effective enough — or, more controversially, cost-effective enough — to be reimbursable. Medical knowledge is constantly evolving, and treatments that seem to lack solid evidence today might seem indispensable tomorrow. Wasteful tests and procedures don't come with labels marked "wasteful," and most patients and providers genuinely believe the care they're getting and giving is necessary.

More at <http://www.time.com/time/politics/article/0,8599,1905340,00.html>

POINTS OF VIEW - III

Administration urged to engage public on e-health records

BY ALIYA STERNSTEIN, *NEXTGOV*

As the Obama administration seeks to determine who uses electronic health records and for what purposes, some health information technology specialists say it is critical that the public provide feedback on the issue. They note it could dictate how billions of economic stimulus dollars are spent.

The 2009 American Recovery and Reinvestment Act allocated about \$20 billion to encourage doctors and hospitals to install e-records systems by 2014. Medical professionals who make "meaningful use" of e-records by 2011 or 2012 would be eligible for up to \$44,000 in Medicare payments spread out over five years. An advisory committee within the Health and Human Services Department met on June 16 to begin defining meaningful use.

While HHS opened the meeting to the public and is seeking comment on proposed recommendations, "they could go further to talk about a variety of different public and consumer uses and sort of their vision for where they want this [process] to go," said Michael W. Painter, senior program officer at the Robert Wood Johnson Foundation, a philanthropic organization that focuses on health issues. For example, a Google consumer health application could meet the meaningful standard and should be discussed in public forums, he said.

"I thought the meeting was excellent and thought-provoking...[but] the vision they come up with and the definitions they create should incorporate a specific role for the public," Painter said.

One predicament might be that federal officials and the public are talking past each other. Americans are weighing in on health care reform via opinion polls, and White House officials have said they want feedback on administration proposals, but the two sides do not have a forum for direct communication, say some health care system critics.

"In my view, there are parallel universes of health care reform discussion. One is what everyday people are saying and thinking. . . .And, yes, the White House hopes people will visit its site on reform and weigh in," said Brian Klepper, managing principal of Florida-based market research firm Healthcare Performance Inc. "The core problem here is that there is no political power center for regular people toglom on to health care reform."

Furthermore, some potential meaningful uses will be more important to patients than providers, insurers, vendors and everyone else getting health IT stimulus funding. Some observers argue that the definition of meaningful use should explicitly grant patients the right to access data entered by physicians or even own it so they can take it and pursue treatment elsewhere.

More at http://www.nextgov.com/nextgov/ng_20090623_2200.php

Personal Profiling

An Interview with Sandra Soo-Jin Lee on Direct-to-Consumer Genomics and Social Networking

BY ANDREW PLEMMONS PRATT,
SCIENCEPROGRESS

Spit in a cup, send it off, and get your genetic profile delivered to your inbox. Direct-to-consumer genetic testing is that simple, right? Maybe, but understanding what it means is far more complex, says bioethicist Sandra Soo-Jin Lee, because much of the research on the connections between our DNA and our health remains uncertain.

But even if the genome-wide association studies that form the basis for these genetic profiles are imprecise, don't consumers still have a right to know about their own genes? Should they expect a certain level of validity for information they're buying? For the moment DTC genetic testing falls, in Lee's words, in a "regulatory no-man's land, with little oversight by federal agencies." And the question remains, do we need health professionals act as gatekeepers and help interpret this new information?

Lee, a medical anthropologist who works as a senior research scholar at the Stanford Center for Biomedical Ethics, and her colleague LaVera Crawley, examined the expanding DTC industry and its implications for consumer health and privacy in an article that appears in the current issue of the American Journal of Bioethics.

Learning about the genes that give you eyes brown brown eyes or make you lactose intolerant is one thing, but some services offer the ability to share your data with others through social networking tools. And not all genetic information is personal. "One of the special qualities of genetic information," explains Lee, "is that it is information about the primary user; but it also information about others who may not have consented or agreed to have that information shared with other individuals." For instance, a heritable trait increasing risk for breast cancer has implications for the person getting tested, as well as their children and grandchildren.

The Genetic Information Non-discrimination Act passed last year promises to protect citizens who might face unfair treatment on account of their DNA, but Lee warns that it's also not yet clear how the legislation will treat the data shared through these social networks.

More at <http://www.scienceprogress.org/2009/06/personal-profiling/>

POINTS OF VIEW - IV

A Pound of Cure

The federal government is about to spend big on health-care IT. Too bad the medical industry has a vested interest in inefficiency.

BY ANDY KESSLER, *TECHNOLOGY REVIEW*

Technology is once again being touted as a cure-all, this time for what ails the American health-care industry. The Obama administration's \$787 billion stimulus plan includes \$19 billion for health-care IT spending that provides incentives for doctors and hospitals to adopt electronic health records. Starting in 2011, stimulus funds will provide additional Medicare and Medicaid reimbursements for health-care providers using such systems.

These federal funding programs assume that the critical hurdle to widespread adoption of electronic medical records is cost. Indeed, hospitals surveyed in a study published last year in the *Journal of the American Medical Association* reported cost as the major barrier. Yet compared with other businesses, the health-care industry has been unmoved by the logic of lowering costs to increase profits. The truth is that these folks could have digitized the whole industry ages ago. The technology has been around for a long time: Wall Street began phasing out physical stock certificates over 35 years ago. Even the cash-strapped airline industry has gone ticketless, removing huge labor and overhead costs. These industries started using electronic records because they believed it would save money. The health-care industry simply has not followed suit.

The reason lies neither with cost nor with inadequate technology. Rather, the health-care industry's reluctance to digitize its records is rooted in a desire to keep medicine's lucrative business model hidden. Dangling \$19 billion in front of a \$2.4 trillion industry is not nearly enough to get it to reveal the financial secrets that electronic health records are likely to uncover—and upon which its huge profits depend. In those medical records lie the ugly truth about the business of medicine: sickness is profitable. The greater the number of treatments, procedures, and hospital stays, the larger the profit. There is little incentive for doctors and hospitals to identify or reduce wasteful spending in medicine.

The amount of unnecessary spending is huge. In a project that analyzed 4,000 hospitals, the Dartmouth College Institute for Health Policy and Clinical Practice estimated that eliminating 30 percent of Medicare spending would not change either access to health care or the quality of the care itself. The Congressional Budget Office then suggested that \$700 billion of the approximately \$2.3 trillion spent on health care in 2008 was wasted on treatments that did not improve health outcomes. This excessive spending has kept the entire health-care industry growing

faster than the population, and faster than inflation, for decades.

While electronic medical records do have sizable up-front costs, they also have the potential to save big, in part by streamlining administrative costs. According to a 2003 article by Dr. Steffie Woolhandler in the *New England Journal of Medicine*, administration accounts for 31 percent of expenses in the U.S. health-care industry, or more than \$500 billion per year. (To put that in perspective, Google has spent well under 10 percent of that on all its R&D.) Richard Hillestad of the Rand Corporation wrote in *Health Affairs*, in 2005, that health-care information technology could save physicians' offices and hospitals more than \$500 billion over 15 years thanks to improvements in safety and efficiency.

Electronic medical records would make it much easier to conduct the studies needed to track down this wasteful spending. According to one estimate, only about 4 percent of U.S. hospitals use comprehensive electronic record systems; most rely on paper records. As a result, analyzing the effectiveness of specific treatments—for example, spinal-fusion surgery versus physical therapy for back pain caused by a herniated disc—is unnecessarily expensive and time consuming. Physicians must compile data for a significant number of patients undergoing each treatment and correlate that information with each patient's outcome.

Using electronic health records, in combination with data mining and search technology, would make this kind of analysis much easier. Patients who fit specific criteria could be identified and tracked automatically, for example. Researchers would be able to analyze larger numbers of patients and a wider variety of treatments. With easy access to this kind of information, wasteful spending could be identified more readily, allowing payers, whether Medicare or private insurers, to stop reimbursing for expensive but unnecessary tests and procedures.

An even bigger threat to the sickness industry's business model is that by allowing automated tracking of patients over time, electronic health records would set the stage for early detection and preventive medicine. Currently, the entire industry is organized around treating sickness, rather than keeping people healthy in the first place. Three-quarters of health-care spending is devoted to chronic care, but the National Cancer Institute and the Centers for Disease Control and Prevention allot just 12 percent of their budgets to research on early detection. Moreover, the payment system is structured around reimbursement for treatment rather than prevention.

With widespread use of electronic health records, it would be easier to expand preventive medicine, not only by educating patients about lifestyle changes but also by conducting mass screenings.

More at http://www.technologyreview.com/printer_friendly_article.aspx?id=22852&channel=computing§ion=

POINTS OF VIEW - V

Great Wall of Facebook: The Social Network's Plan to Dominate the Internet — and Keep Google Out

BY FRED VOGELSTEIN, *WIRED*

Larry Page should have been in a good mood. It was the fall of 2007, and Google's cofounder was in the middle of a five-day tour of his company's European operations in Zurich, London, Oxford, and Dublin. The trip had been fun, a chance to get a ground-floor look at Google's ever-expanding empire. But this week had been particularly exciting, for reasons that had nothing to do with Europe; Google was planning a major investment in Facebook, the hottest new company in Silicon Valley.

Originally Google had considered acquiring Facebook—a prospect that held no interest for Facebook's executives—but an investment was another enticing option, aligning the Internet's two most important companies. Facebook was more than a fast-growing social network. It was, potentially, an enormous source of personal data. Internet users behaved differently on Facebook than anywhere else online: They used their real names, connected with their real friends, linked to their real email addresses, and shared their real thoughts, tastes, and news. Google, on the other hand, knew relatively little about most of its users other than their search histories and some browsing activity.

But now, as Page took his seat on the Google jet for the two-hour flight from Zurich to London, something appeared to be wrong. He looked annoyed, one of his fellow passengers recalls. It turned out that he had just received word that the deal was off. Microsoft, Google's sworn enemy, would be making the investment instead—\$240 million for a 1.6 percent stake in the company, meaning that Redmond valued Facebook at an astonishing \$15 billion.

As the 767 took off, Page tersely but calmly shared the news with the others on the plane and answered their questions for about 15 minutes. "Larry was clearly, clearly unhappy about it," the passenger says.

Page soon got over it, but Facebook's rejection was still a blow to Google; it had never lost a deal this big and this publicly. But according to Facebookers involved in the transaction, Mountain View never had much of a chance—all things being equal, Microsoft was always the favored partner. Google's bid was used primarily as a stalking horse, a tool to amp up the bidding. Facebook executives weren't leaping at the chance to join with Google; they preferred to conquer it. "We never liked those guys," says one former Facebook engineer. "We all had that audacity, 'Anything Google does, we can do better.' No one talked about MySpace or the other social networks. We just talked about Google."



Today, the Google-Facebook rivalry isn't just going strong, it has evolved into a full-blown battle over the future of the Internet—its structure, design, and utility. For the last decade or so, the Web has been defined by Google's algorithms—rigorous and efficient equations that parse practically every byte of online activity to build a dispassionate atlas of the online world. Facebook CEO Mark Zuckerberg envisions a more personalized, humanized Web, where our network of friends, colleagues, peers, and family is our primary source of information, just as it is offline. In Zuckerberg's vision, users will query this "social graph" to find a doctor, the best camera, or someone to hire—rather than tapping the cold mathematics of a Google search. It is a complete rethinking of how we navigate the online world, one that places Facebook right at the center. In other words, right where Google is now.

All this brave talk might seem easy to dismiss as the swagger of an arrogant upstart. After all, being Google is a little like being heavyweight champion of the world—everyone wants a shot at your title. But over the past year, Facebook has gone from glass-jawed flyweight to legitimate contender. It has become one of the most popular online destinations. More than 200 million people—about one-fifth of all Internet users—have Facebook accounts. They spend an average of 20 minutes on the site every day. Facebook has stolen several well-known Google employees, from COO Sheryl Sandberg to chef Josef Desimone; at least 9 percent of its staff used to work for the search giant. And since last December, Facebook has launched a series of ambitious initiatives, designed to make the social graph an even more integral part of a user's online experience. Even some Googlers concede that Facebook represents a growing threat. "Eventually, we are going to collide," one executive says.

More at http://www.wired.com/techbiz/it/magazine/17-07/ff_facebookwall

INTERNET GOVERNANCE

Web Pries Lid of Iranian Censorship

BY BRIAN STELTER AND BRAD STONE,
THE NEW YORK TIMES

Shortly after Neda Agha-Soltan bled her life out on the Tehran pavement, the man whose 40-second video of her death has ricocheted around the world made a somber calculation in what has become the cat-and-mouse game of evading Iran's censors. He knew that the government had been blocking Web sites like YouTube and Facebook. Trying to send the video there could have exposed him and his family.

Instead, he e-mailed the two-megabyte video to a nearby friend, who quickly forwarded it to the Voice of America, the newspaper *The Guardian* in London and five online friends in Europe, with a message that read, "Please let the world know." It was one of those friends, an Iranian expatriate in the Netherlands, who posted it on Facebook, weeping as he did so, he recalled.



Copies of the video, as well as a shorter one shot by another witness, spread almost instantly to YouTube and were televised within hours by CNN. Despite a prolonged effort by Iran's government to keep a media lid on the violent events unfolding on the streets, Ms. Agha-Soltan was transformed on the Web from a nameless victim into an icon of the Iranian protest movement.

At one time, authoritarian regimes could draw a shroud around the events in their countries by simply snipping the long-distance phone lines and restricting a few foreigners. But this is the new arena of censorship in the 21st century, a world where cellphone cameras, Twitter accounts and all the trappings of the World Wide Web have changed the ancient calculus of how much power governments actually have to sequester their nations from the eyes of the world and make it difficult for their own people to gather, dissent and rebel.

Iran's sometimes faltering attempts to come to grips with this new reality are providing a laboratory for what can and cannot be done in this new media age — and providing lessons to other governments, watching with calculated interest from afar, about what they may be able to get away with should their own citizens take to the streets.

One early lesson is that it is easier for Iranian authorities to limit images and information within their own country than it is to stop them from spreading rapidly to the outside world. While Iran has severely restricted Internet access, a loose worldwide network of sympathizers has risen up to help keep activists and spontaneous filmmakers connected.

The pervasiveness of the Web makes censorship "a much more complicated job," said John Palfrey, a co-director of Harvard's Berkman Center for Internet and Society.

The Berkman Center estimates that about three dozen governments — as widely disparate as China, Cuba and Uzbekistan — extensively control their citizens' access to the Internet. Of those, Iran is one of the most aggressive. Mr. Palfrey said the trend during this decade has been toward more, not less, censorship. "It's almost impossible for the censor to win in an Internet world, but they're putting up a good fight," he said.

Since the advent of the digital age, governments and rebels have dueled over attempts to censor communications. Text messaging was used to rally supporters in a popular political uprising in Ukraine in 2004 and to threaten activists in Belarus in 2006. When Myanmar sought to silence demonstrators in 2007, it switched off the country's Internet network for six weeks. Earlier this month, China blocked sites like YouTube to coincide with the 20th anniversary of the Tiananmen Square crackdown.

In Iran, the censorship has been more sophisticated, amounting to an extraordinary cyberduel. It feels at times as if communications within the country are being strained through a sieve, as the government slows down Web access and uses the latest spying technology to pinpoint opponents. But at least in limited ways, users are still able to send Twitter messages, or tweets, and transmit video to one another and to a world of online spectators.

Because of the determination of those users, hundreds of amateur videos from Tehran and other cities have been uploaded to YouTube in recent days, providing television networks with hours of raw — but unverified — video from the protests.

The Internet has "certainly broken 30 years of state control over what is seen and is unseen, what is visible versus invisible," said Navtej Dhillon, an analyst with the Brookings Institution.

More at http://www.nytimes.com/2009/06/23/world/middleeast/23censor.html?_r=1&partner=rss&emc=rss

INTERNET GOVERNANCE - II

The rise of Hate 2.0

The number of hate and terrorist websites has increased by a third in the past year, according to the Simon Wiesenthal Center.

BY DANIEL EMERY, *BBC*

The Los Angeles-based Jewish human rights organisation put the figure at more than 8,000 in its 2008 report Hate 2.0. It said the presence of such sites "demeans and threatens African Americans, Jews, immigrants, gays and virtually every religious denomination".

And the number of so-called hate sites is growing fast, while the use of social networks to push controversial messages is also on the rise.

In May this year, Facebook became embroiled in a row after a number of Holocaust denial groups were set up on the site.

Critics said Facebook was propagating anti-Semitism, others said that free speech was a cornerstone of society and Facebook should keep its hands off.

At the time, Barry Schnitt, a spokesman for Facebook, said it should be "a place where controversial ideas can be discussed".

"The bottom line is that, of course, we abhor Nazi ideals and find Holocaust denial repulsive and ignorant," he said.

"However, we believe people have a right to discuss these ideas."

A few days later, the site had closed two of the groups, Holocaust is a Holofoax and Based on the facts... there was no Holocaust. It said they had breached the firm's terms of service.

But there are still plenty of other Holocaust denial groups on Facebook: Holocaust is a Myth, 6,000,000 for the TRUTH about the Holocaust, The problem of forged Holocaust photos, and Holocaust Deniers, to name just four.

Denial outlawed

In a visit to the Buchenwald concentration camp in June this year, President Barack Obama criticised Iranian President Mahmoud Ahmadinejad, who had called the Holocaust a "great deception".

"To this day we know there are those who insist the Holocaust never happened, a denial of a fact or truth that is baseless, ignorant and hateful," Mr Obama said in a brief address.

Holocaust denial is illegal in 13 countries, including France,

Germany and Israel. It was also a crime in Slovakia, although this law was repealed in May 2005.

The Netherlands, Denmark, Sweden, Italy, and the United Kingdom have all rejected Holocaust denial legislation.

In Europe, citizens are covered by the European Convention on Human Rights which states: "Everyone has the right to freedom of expression."

But it adds that governments can restrict free speech, among other reasons, in the interests of national security, to preserve public safety and for the prevention of disorder or crime.

Rabbi Abraham Cooper, associate dean of the Simon Wiesenthal Center, told the BBC that it was not a freedom of speech issue.

"Holocaust denial is a perfect example of how a hateful idea was incubated on the internet. It promotes hatred, it promotes violence and it's a kind of precursor to genocide.

"It's not the idea that needs to be scrubbed; it's fact that the internet elevates crackpot theories to a level it doesn't deserve.

"These sites aren't about the discussion of ideas; they are about getting people to subscribe to the ideal of hate."

But speaking to the BBC, Douglas Murray, director of think tank The Centre for Social Cohesion, said that society should be able to accept any point of view, even if that view was proven to be false.

"You have to allow different opinions, even lies, as long as they don't incite violence. Otherwise what is true becomes dogma and then becomes incapable of being defended," he said.

White power

In 1995 Don Black founded Stormfront - a white supremacist website seen by many as the internet's first "major hate site", although it had existed as a bulletin board for a number of years prior to that.

In May he was one of 22 individuals excluded from the United Kingdom by the Home Office for "promoting serious criminal activity and fostering hatred that might lead to inter-community violence".

He told the BBC that - in America - people could say and think whatever they liked.

More at <http://news.bbc.co.uk/2/hi/technology/8097979.stm>

INTERNET GOVERNANCE - III

New call for ICANN to be privatised *The world's regional Internet registries (RIRs) have added their weight to call for Internet governance to be privatised.*

BY MAXWELL COOTER, *COMPUTERWORLD*

The world's regional Internet registries (RIRs) have added their weight to call for Internet governance to be privatised.

The RIRs have followed the European Union's demand, proposed by European Commissioner Viviane Reding last month, for the ending of the collaboration agreement between ICANN and the US Department of Commerce.

The RIRs, responsible for IP address allocation within geographic regions, have put out a joint statement saying that it was time for the US government to pull out of control of the Internet: the Internet Domain Name System (DNS) is currently managed by ICANN and the US Department of Commerce under an agreement set to expire on 30 September.

Axel Pawlik, managing director of European RIR, RIPE NCC, told Techworld that there was no cohesion between the EU call and the RIRs' position. "We didn't confer with each other, we seen several ideas from the EU, some of which that we thought we were good, but

there's no question of this being coordinated in any way.

Pawlik stressed that all the RIRs - including the north American registry, ARIN, were in full agreement on this issue. He also made it plain that the RIRs had no complaints about the way that ICANN was run, merely the problems that Internet governance structure caused.

"It's purely a political issue," he said. "We have an excellent opinion of ICANN based on the way that it runs things, but it's the political dimension can cause problems," he said.

The RIRs said that the existing Governmental Advisory Committee (GAC) should be given great power. "It's purely advisory at the moment," said Pawlik, "there are some countries - notably China - that don't get involved but the GAC could be taken more seriously, giving stakeholders a greater say." He also said that European Commissioner Reding's idea of a G-12 for Internet governance was an interesting idea "but we'd still be arguing as to who the 12 countries would be in 50 years' time."

However, Pawlik is realistic enough to know that the US is not going to give up control of ICANN lightly. "They asked for comments and we've made our views known," he said. "But even with the change of administration, I can't see them loosening that control," he added.

More at <http://news.idg.no/cw/art.cfm?id=128E5BEC-1A64-67EA-E42EDD561D4146F3>

EU lays out plans for the "internet of things"

What will you do when your yoghurt pot starts talking to you? Mass RFID deployment on consumer products prompts EU to prepare legislation

BY DAVE BAILEY, *V3*

The European Commission has announced plans for Europe to play a leading part in developing and managing interconnected networks formed from everyday objects with radio frequency identity (RFID) tags embedded in them - the so-called "internet of things".

The Commission has launched a 14-point action plan to address the issues raised from such widespread interconnectivity.

"New examples of applications that connect objects to the internet and each other are created [everyday]: from cars connected to traffic lights that fight congestion, to home appliances connected to smart power grids and energy

metering that allows people to be aware of their electricity consumption," said EU Commissioner for Information Society and Media Viviane Reding.

The EC expects there will be a progressive connection of a variety of physical objects, and not just computers - creating the 'internet of things'. These could be everyday items such as food packaging that records the temperature along its supply chain, or different prescription drugs that warn patients of a possible incompatibility.

To meet the challenges raised by such interconnected objects, the EU's action plan aims to help "Europeans benefit from this evolution and at the same time address the challenges it raises such as privacy, security and the protection of personal data," according to the Commission.

The plan's major concerns are related to governance, privacy, data protection and the emerging risks which could potentially surface as new RFID technology is rolled out into ever-more consumers devices and products.

More at <http://www.v3.co.uk/computing/news/2244448/eu-prepares-mass-rfid>

NEXT WEEK

JUNE 29TH - JULY 2, 2009

Symposium on Health IT Funding, EHR Implementation. Participants will hear from the policy leaders responsible for many of the programs within the federal government, as well as nationally recognized experts on topics such as privacy, financing, standards, and technical assistance. Location: Marriott Boston Cambridge. Details at: <http://www.hitsymposium.com/>

JUNE 30TH, 2009

12:15 - 1:30 PM. The Federal Communications Commission (FCC) will host a brown bag lunch titled "Bridging the Gap: Transactions 101 -- An Introduction to Communications Transactions and Related FCC Oversight". For more information, contact Sarah Reiser at spreiser@hhlaw.com. The Federal Communications Bar Association (FCBA) states that this is a FCBA event. Location: Hogan & Hartson, 555 13th St, NW.

JUNE 30TH, 2009

2:00 PM EST. HISPC Seminar on Health IT Agreements. This presentation will discuss the national relevance for the development and implementation of DSAs, the process used by the IOA collaborative for developing the model agreements, as well as an overview of the pilot projects used to test the model DSAs. Location: Online. Details at: <http://shorl.com/sobubogrulali>

JUNE 30TH, 2009

Innovation in Care Through Telehealth and IT Strategies. Join us for a challenging and engaging discussion of innovation in healthcare that will cover topics ranging from Second Life to Healthcare stimulus and reform, and from Telemedicine to gaming technology. Location: San Leandro, CA. Details at: <http://www.himss.org/asp/ContentRedirector.asp?ContentId=69298&cetID=500>

June						
Sun	Mon	Tues	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4

Featured Conference of the Week

**Personal Democracy Forum Conference
Technology is changing politics**

June 29th - 30th, 2009

<http://personaldemocracy.com/pdf-conference/personal-democracy-forum-conference>

The Personal Democracy Forum is the world's largest and best known conference on the intersection of technology and politics. For the sixth year, more than 1,000 top opinion makers, political practitioners, technologists and journalists will come together to network, exchange ideas, and explore how technology and the Internet are changing politics, democracy, and society.

SITES COMPENDIUM

www.archinte.ama-assn.org
www.boston.com
www.bostonreview.net
www.cdt.org
www.earthtimes.org
www.ec.europa.eu
www.ews.idg.no
www.fcw.com
www.healthnewsdigest.com
www.jmir.org
www.latimes.com
www.news.bbc.co.uk
www.newswise.com
www.nextgov.com
www.nytimes.com
www.out-law.com
www.papers.ssrn.com
www.personaldemocracy.com
www.scienceprogress.org
www.technologyreview.com
www.time.com
www.v3.co.uk
www.washingtonpost.com
www.wiesenthal.com
www.wired.com
www.yaleglobal.yale.edu



RESEARCH@MARKLE.ORG

Research & Selection: Stefaan Verhulst
Production: swandivedigital

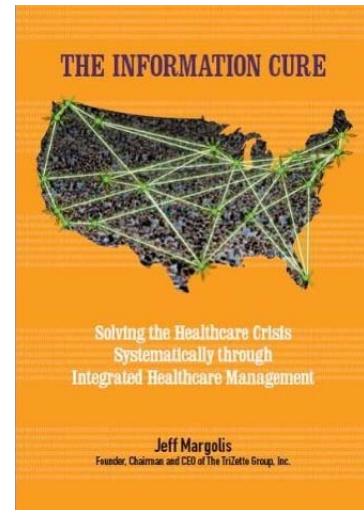
Please send your questions, observations and suggestions to sverhulst@markle.org

The views expressed in the Weekly Digest do not necessarily reflect those of the Markle Foundation.

BOOK NOTICE**THE INFORMATION CURE**

By Jeff Margolis

SAN DIEGO, Calif. – The Information Cure provides a unique, simplified perspective that anyone can understand about how our U.S. healthcare system really works and introduces a new, comprehensive model that combines thoughtful and practical systematic design and information technology to substantially improve the value and effectiveness of the healthcare industry. Solving the Healthcare Crisis Systematically Through Integrated Healthcare Management, the book debuted at the 2009 Institute of America's Health Insurance Plans in San Diego and is available at www.informationcure.com and Amazon.com. Every constituent who is part of the American healthcare supply chain should find this 155- page book an easy and informative read, including consumers, physicians, hospital system executives, brokers and employers.



"We are publishing The Information Cure at a critical time because the book offers some important solution approaches that are supportive of and relevant to today's healthcare reform discussion," said Margolis. "First, Integrated Healthcare Management (IHM) proposes a new framework for systematically organizing our healthcare system by more fully integrating available benefits information with available care information on behalf of healthcare consumers to create an affordable and sustainable U.S. healthcare model that drives the greatest value for each healthcare dollar spent.

More at: http://www.healthnewsdigest.com/news/Book_Review_440/The_Information_Cure.shtml