



### eHealth Initiative Survey Links Health IT to Lower Costs and Improved Outcomes

PRNEWSWIRE

WASHINGTON, Sept. 11 /PRNewswire-USNewswire/ -- The exchange of health information electronically between physicians, hospitals, health plans, and patients is decreasing the cost of care and improving outcomes, according to a new survey released by the non-profit eHealth Initiative today. The 2008 Fifth Annual Survey of Health Information Exchange at the State and Local Levels, which included responses from 130 community-based initiatives in 48 states, shows the significant impact fully operational initiatives are having on improving health care delivery and efficiency.

The key findings from the 2008 survey are as follows:

- A majority (69%) of the fully operational exchange efforts (29/42) report reductions in health care costs. These respondents say health information exchange allows them to:
  - Decrease dollars spent on redundant tests
  - Reduce the number of patient admissions to hospitals for medication errors, allergies or interactions
  - Decrease the cost of care for chronically ill patients - Reduce staff time spent on administration
- About half (52%) of fully operational exchange efforts (22/42) report positive impacts on health care delivery, including:
  - A decrease in prescribing errors - Improved access to test results - Improved compliance with chronic care and prevention guidelines - Better care outcomes for patients - Increased recognition of disease outbreaks - Improved quality of practice life - Reductions in malpractice insurance costs
- In addition to improving care delivery, tackling population health challenges continues to be a goal of many operational health information exchange efforts with ten offering disease or chronic care management services, eight offering quality improvement reporting for clinicians, six offering public health reporting, and five offering quality improvement reporting for purchasers or payers. .

More at: [http://www.redorbit.com/news/health/1551922/ehealth\\_initiative\\_survey\\_links\\_health\\_it\\_to\\_lower\\_costs\\_and/](http://www.redorbit.com/news/health/1551922/ehealth_initiative_survey_links_health_it_to_lower_costs_and/)

#### Inside this issue:

- Health IT .....2**
- Information Sharing .....4**
- Privacy and ID .....5**
- New Reports and Papers .....7**
- Points of View .....13**
- Internet Governance .....16**
- Book Review .....19**

#### FIGURES OF THE WEEK

- Parks Associates estimates that global online revenues from games played on consoles will grow from \$1.3 bln in 2008 (mostly from Xbox Live) to more than \$8 bln in 2013.
- Across the 17 global markets surveyed, 42% of people know what online social networking is, says Synovate. The Dutch were most likely to know the term with 89% answering 'yes', followed by Japan at 71% and Americans with 70% answering in the affirmative. 26% across the markets surveyed are members of social networking sites. This peaked with the Netherlands at 49%, United Arab Emirates (UAE) at 46%, Canada at 44% and the US at 40% (though keep in mind that's 40% of a huge population).
- Online TV viewing has been gaining in popularity. 20% of American households who use the internet watch television broadcasts online, double the viewership from 2006, The Conference Board reports. The top two destinations for online broadcasts are the official TV channel homepage and YouTube.com.

## HEALTH IT

### Entrepreneurial docs succeed with business help

BY BARBARA KIRCHHEIMER,  
*MODERN HEALTHCARE*

There are a dizzying number of information technology products targeting physicians and hospitals, and each day seems to bring more to the market. Some of them are created by frustrated physicians who want to find solutions that will help others like themselves.

The skills that make a good doctor do not always transfer smoothly to the business world, and yet some of these doctors happily trade in their white coats for suits and ties. Those who have succeeded in making the transition from examination room to corner office, however, seem to agree on one thing: Doctors should stick to what they do and know best and leave other aspects of running a business to those with formal business training.

Woodrow Gandy and Rob Langdon have followed this model. The two practiced together as board-certified emergency physicians before starting up their charting solutions company, T-System, in 1996 in Dallas. "We were seeing rising emergency department volumes, we were experiencing pressures from the hospital to see patients more quickly, and at the same time had increasingly burdensome regulations," Langdon said. "We developed a set of paper templates to be used at the bedside to be able to chart more rapidly."

Their goal was to provide hospitals, physicians and nurses with a documentation system that would allow them to spend more time at the patient's bedside, cut down on the amount of time and cost spent on handwritten charts and transcription, and also enhance compliance with reimbursement and regulatory requirements. "The reason for our interest in starting a company was our recognition that there were some huge problems that we faced and other emergency physicians faced in practicing," Gandy said. Neither Gandy nor Langdon has an MBA, although Gandy says that they received their business degrees from the "school of hard knocks," thanks to their prior experience managing their own physician group and starting up a medical billing company. But as their company has grown over the years, the two have increasingly delegated authority, hiring a chief financial officer five years ago and a chief executive officer about two years ago. Each currently holds the title of co-founder and co-chairman.

Twelve years after its launch, T-System brings in \$55 million annually in revenue, Gandy said, and its paper template system is used by 42% of U.S. emergency departments, according to the company's Web site. A spokeswoman said

it has been a profitable venture since its inception, although she declined to provide a specific figure. The company also has paper systems for emergency nurses, urgent-care centers and primary-care offices. In addition to the paper systems, T-System offers a computerized emergency department information system that has 166 hospital clients, about half of whom had used its paper templates before going electronic. It employs 235 people, including some 50 doctors and nurses.

"In the typical physician-started companies, doctors have a problem," Langdon said. "They're used to being in complete control and not used to giving up power in the decisionmaking area." Bringing in a leadership team and trusting them to make good choices has "really allowed us to reach many of the successes we've had," he said. Langdon was happy to trade in the physical challenges of emergency medicine for the more controlled environment of the business world, he said.

Gandy said he sometimes misses the excitement of practicing emergency medicine but that he doesn't regret his decision to leave it behind for the business world. But some physicians who start their own ventures choose not to give up their day jobs. Richard Chesbrough, the CEO of RADAR Medical Systems, which he founded with a partner in 2005, still practices radiology and spends about 80% of his time in clinical practice. Since 2000, when he developed a medical device used in breast biopsies, he has had one foot in medicine and the other in entrepreneurship.

A practicing radiologist since 1991, Chesbrough began doing medical legal reviews in the mid-1990s in which defense attorneys would ask him to help defend their clients in radiology malpractice cases. Over the next decade, he saw a shift in the types of cases he was getting. At first, most of the lawsuits were the result of a radiologist misreading a scan. But over the years, the focus began to shift to "fumbled handoffs," where the correct finding was made but the information somehow didn't get back to the referring physician or patient.

In 2005, he founded RADAR with Jack Cornell, who is the company's president and holds an MBA from the Wharton School of the University of Pennsylvania. The company is based in Bingham Farms, Mich., in the metro Detroit area, while Cornell maintains an office in Ohio. RADAR officially launched several months ago and now has two test sites up and running, Chesbrough said.

More at <http://www.modernhealthcare.com/apps/pbcs.dll/article?AID=/20080908/REG/309089992/1029/FREE&nocache=1&nocache=1>

## HEALTH IT - II

### Broad coalition pushes for quick action on health IT

BY ANDREW NOYES, *CONGRESS DAILY*

With Congress looking to wrap up its legislative year, industry and nonprofit groups that have pushed for passage of legislation to create a nationwide system of electronic health records are turning up the heat on Capitol Hill.

More than 175 stakeholders, including the American Cancer Society, American Heart Association, AstraZeneca, Cisco Systems, and Pfizer will send a letter to members of the House and Senate today hoping to spur action.

"Our organizations all share the downstream effects of our inefficient healthcare system, particularly rising healthcare costs," states the letter from the Health IT Now Coalition, which will be unveiled at a morning briefing.

The signatories, who believe technology can improve quality of and access to patient care and reduce medical errors and costs, warn against waiting for "the uncertainty of the priorities of a new administration" to move legislation they say has wide bipartisan support.

Bills pending in both chambers have won the group's endorsement but have rankled privacy advocates. Broadly,

those measures would create a public-private process to determine standards for interoperability, product certification, quality measures and an accelerated process for standards improvement and would provide financial incentives for healthcare providers to adopt and use health IT. The bills include text to encourage patient and provider education, as well as privacy and security protections.

Senate Health, Education, Labor and Pensions Chairman Edward Kennedy and ranking member Michael Enzi introduced a bill more than a year ago and it was hotlined before the August recess. The threat of holds by several members delayed voting on the measure.

In the House, a bill by Energy and Commerce Chairman John Dingell and ranking member Joe Barton is awaiting floor action, while Ways and Means Health Subcommittee Chairman Fortney (Pete) Stark, D-Calif., is working on a proposal that would use Medicare reimbursement as an incentive for healthcare providers.

Stark is expected to introduce his bill this week, Health IT Now Executive Director Joel White said Monday, citing the "great desire" by Stark and Health Subcommittee ranking member Dave Camp, R-Mich., to move ahead with legislation.

More at [http://www.nextgov.com/nextgov/ng\\_20080909\\_4256.php](http://www.nextgov.com/nextgov/ng_20080909_4256.php)

### Managing Risks in Health 2.0

BY NEIL VERSEL,

*DIGITAL HEALTH CARE & PRODUCTIVITY*

Interactive media with user-generated content, often generically referred to as Web 2.0, has taken off in health care in the last couple of years. But with all the options and convenience that blogs, wikis, social networking sites, chat rooms, and message boards have opened up for patients and providers alike, the technology known as health 2.0 or medicine 2.0 is not without risk.

"This opens up a multitude of opportunities for patients," Kevin Clauson, associate professor of pharmacy practice and a specialist in drug information at Nova Southeastern University (Palm Beach Gardens, Fla.), said here Friday at the first Medicine 2.0 Congress, which attracted 180 people from 19 countries for an academic-level discussion on interactive health-IT. He noted that PatientsLikeMe has become a popular forum and virtual support group for those with serious health issues.

Health 2.0 also can open up organizations to embarrassment or possibly even legal liability when it comes to interaction

between patients and practitioners. Clauson noted that pharmacists in the U.S. have a "duty to warn" if patients are put in potentially unsafe situations. But it is not clear, Clauson said, if this duty extends to patient-posted content that may indicate that person is taking drugs that may interact with each other.

As more providers move to electronic health records and personal health records that patients can view, the public might be surprised to learn that clinicians have their own form of derogatory slang. Clauson said some popular descriptions he has seen in medical charts include: "CLL" ("chronic low-life"), "LOBNH" ("lights on but nobody home"), and "grave dodger" to describe a chronically ill elderly patient. What happens if patients suddenly start reading such language?

Messages often do get muddled online. E-mails and blogs are wide open to misinterpretation, since it is difficult to communicate tone in typed text. "Poor communication is exacerbated by writing because most people don't write very well," Clauson added.

Sometimes, organizations may get hurt by poor judgment that is completely beyond their institutional control.

More at <http://www.digitalhcp.com/2008/09/09/health20risk.html>

## INFORMATION SHARING

### Intelligence Cell Defends Cyberspace

BY MARYANN LAWLOR, *REDORBIT*

Analysts' expertise defines cyberthreats. A small yet dedicated cadre of network and intelligence experts is helping keep the U.S. Army's network safe in Europe -and by extension, world-wide-by ferreting out the bad guys in Cyberspace. This unique group of civilian soldiers characterizes the threat by examining how adversaries ping and attempt to infiltrate networks, and then it seeks to find their motives. Rather than simply identifying the techniques enemies employ, the group provides the service with the context surrounding attacks so cyberwarriors are better prepared to defend the Army's information infrastructure.

The Cyber-Threat Intelligence Cell is part of the 5th Signal Command under the auspices of U.S. Army Europe, Mannheim, Germany, but the seeds for the cell were sown at U.S. European Command (EUCOM). A group of analysts at the combatant command began recommending information condition changes based on threats, adjusting the condition level of networks in much the same way that changes to force protection take place. This became the foundation of EUCOM's Network Warfare Center, which was created in 2005 and comprised representatives from the intelligence; operations; and command, control, communications and computers sectors.

While visiting the center, Col. William H. Brady, USA, the 5th Signal Command's G-2 at the time, saw the value in analyzing network threat conditions and decided that his organization,

which is essentially the network command for the Army in Europe, could use the same insights. Upon returning to the 5th Signal Command, he began the process to establish the Cyber-Threat Intelligence Cell.

Robert Hembrook, the current deputy G-2 at 5th Signal Command, was working for the J-2 at EUCOM when Col. Brady visited the combatant command and was part of the command's group analyzing network threat conditions. Hembrook now oversees the 5th Signal Command's Cyber-Threat Intelligence Cell, which today comprises two Army civilians and one contractor. Eventually, the staff will consist of four Army civilians and one contractor; he adds, with an even mix of intelligence analysts and network experts.

Soldiers are not part of the cell because they do not possess the skills, Hembrook notes. "There is no MOS [military occupational specialty] that teaches what we do. Cell members have all built their skills and characteristics out of their own knowledge and abilities, and they have an aptitude for it. There is no place that you can go to learn this," he says.

While network defenders explore the who, what, where and when of a network attack, members of the Cyber-Threat Intelligence Cell try to figure out the why, Hembrook explains. The group analyzes incidents and other data and then characterizes patterns of information.

More at [http://www.redorbit.com/news/technology/1548278/intelligence\\_cell\\_defends\\_cyberspace/](http://www.redorbit.com/news/technology/1548278/intelligence_cell_defends_cyberspace/)

### GAO: SBInet strategy needs reworking

BY ALICE LIPOWICZ, *FCW.COM*

The Homeland Security Department needs to immediately change its approach to managing technology in its SBInet border surveillance system to reduce the risks of going over budget and failing to deliver results, a director of the Government Accountability Office testified today.

"It is imperative that the department immediately re-evaluate its plans and approach in relation to the status of the system and related development, acquisition and testing activities," Randolph Hite, director of information technology architecture and system issues at GAO, told the House Homeland Security Committee.

The Secure Border Initiative Network is designed to use cameras, radars, sensors and communications equipment strung on towers. The data from the sensors is fed into a common operating picture computer application at a U.S. Customs and

Border Protection operations center, where border patrol agents can obtain additional input from the sensors and communicate with field agents. The goal is to maximize the capabilities of the border patrol.

Problems with the system identified by the GAO include poor management of requirements development, lack of alignment for those requirements, and lack of definition and benchmarks for the SBInet technology testing program, Hite said.

For example, a test management strategy was not drafted until May and is not final, Hite said. Also, the strategy does not have a master schedule for SBInet testing, metrics for measuring testing progress, or a clear definition of testing roles and responsibilities, he said.

DHS officials agreed with seven of the GAO's eight recommendations to address the problems, leading Hite to conclude that improvements are likely to be implemented. "I am cautiously optimistic going forward," Hite testified.

More at <http://www.fcw.com/online/news/153745-1.html>

## PRIVACY AND ID

### Libertarian Barr, EPIC Outline Privacy Agenda

BY GRANT GROSS, *IDG NEWS SERVICE*

The Democratic and Republican candidates for U.S. president aren't giving enough emphasis to privacy and civil rights issues, the Electronic Privacy Information Center (EPIC) and Bob Barr, the Libertarian candidate for president, said Friday.

Privacy issues received no mention at the Democratic and Republican national conventions during the past two weeks, said Barr, a former Republican congressman from Georgia, speaking at an EPIC press conference. Debates about privacy and civil rights issues, including government surveillance of U.S. residents and routine searches of laptops at U.S. borders, were "nowhere to be seen" at the conventions, Barr said.

Barr spoke during the launch of a new EPIC campaign called Privacy '08. The goal is to make privacy issues a larger part of the campaign debate and to educate voters about privacy issues, said Marc Rotenberg, EPIC's executive director. "We need to have this debate," he said.

Barr called on the next president to rein in government surveillance of U.S. residents and called on Congress to update privacy laws by limiting what private businesses can do with person-

al data. Libertarians generally oppose new laws and new regulations, but Barr said limitations on the use of personal information are needed.

Both Republican candidate Senator John McCain of Arizona and Democratic candidate Senator Barack Obama of Illinois supported a bill, passed by Congress in July, that updated the nation's wiretap and surveillance laws. The legislation allows U.S. spy agencies in some cases to intercept the phone calls and e-mails of U.S. residents, based on a suspicion that the person they're communicating with is connected to terrorists.

Barr called the surveillance bill "breathtaking expansion" of the U.S. government's power to spy on residents.

A recent housing finance industry bailout bill required a fingerprint registry for housing lenders, Barr added. "I do give these folks [in Congress] credit for great imagination for the number of new databases they come up with," Barr said.

Both McCain and Obama have included privacy issues in policy statements. "Americans will fully embrace new technologies ... only when they are confident that these new advances can be used safely and securely," McCain's Web site says.

More at [http://www.pcworld.com/businesscenter/article/150754/libertarian\\_barr\\_epic\\_outline\\_privacy\\_agenda.html](http://www.pcworld.com/businesscenter/article/150754/libertarian_barr_epic_outline_privacy_agenda.html)

### Brave New World of Digital Intimacy

BY CLIVE THOMPSON, *NEW YORK TIMES*

On Sept. 5, 2006, Mark Zuckerberg changed the way that Facebook worked, and in the process he inspired a revolt.

Zuckerberg, a doe-eyed 24-year-old C.E.O., founded Facebook in his dorm room at Harvard two years earlier, and the site quickly amassed nine million users. By 2006, students were posting heaps of personal details onto their Facebook pages, including lists of their favorite TV shows, whether they were dating (and whom), what music they had in rotation and the various ad hoc "groups" they had joined (like "Sex and the City" Lovers). All day long, they'd post "status" notes explaining their moods — "hating Monday," "skipping class b/c i'm hung over." After each party, they'd stagger home to the dorm and upload pictures of the soused revelry, and spend the morning after commenting on how wasted everybody looked. Facebook became the de facto public commons — the way students found out what everyone around them was like and what he or she was doing.

But Zuckerberg knew Facebook had one major problem: It required a lot of active surfing on the part of its users. Sure, every day your Facebook friends would update their profiles with some new tidbits; it might even be something particularly

juicy, like changing their relationship status to "single" when they got dumped. But unless you visited each friend's page every day, it might be days or weeks before you noticed the news, or you might miss it entirely. Browsing Facebook was like constantly poking your head into someone's room to see how she was doing. It took work and forethought. In a sense, this gave Facebook an inherent, built-in level of privacy, simply because if you had 200 friends on the site — a fairly typical number — there weren't enough hours in the day to keep tabs on every friend all the time.

"It was very primitive," Zuckerberg told me when I asked him about it last month. And so he decided to modernize. He developed something he called News Feed, a built-in service that would actively broadcast changes in a user's page to every one of his or her friends. Students would no longer need to spend their time zipping around to examine each friend's page, checking to see if there was any new information. Instead, they would just log into Facebook, and News Feed would appear: a single page that — like a social gazette from the 18th century — delivered a long list of up-to-the-minute gossip about their friends, around the clock, all in one place. "A stream of everything that's going on in their lives," as Zuckerberg put it.

More at [http://www.nytimes.com/2008/09/07/magazine/07awareness-t.html?\\_r=3&oref=slogin&pagewanted=print](http://www.nytimes.com/2008/09/07/magazine/07awareness-t.html?_r=3&oref=slogin&pagewanted=print)

## PRIVACY AND ID - II

### Law prof warns against coming ISP privacy apocalypse

BY NATE ANDERSON, *ARS TECHNICA*

Anyone who reads Ars knows that we have concerns about ISP monitoring and the deep packet inspection that often goes along with it, but Colorado Law School prof Paul Ohm takes these worries to the next level—then hauls them thirty floors up in the elevator, climbs the dingy stairway to the roof, and scales the attached cell phone tower. According to Ohm's new paper, ISP use of deep packet inspection gear could well lead to "the greatest reduction of user privacy in the history of the Internet, and users will suffer dire harms."

Be warned, all ye who enter here: Ohm's paper is so depressing that you may need to cope by intravenously administering large quantities of lolcat directly to the bloodstream.

#### The bad news

The basic arguments are ones we've made repeatedly (as shown by Ohm's repeated Ars footnotes), but Ohm makes a powerful case for the dangers of ISP filtering based on the staggering amount of personal and private information they routinely have access to.

"In modern connected life," he writes, "almost no other entity poses a greater threat to privacy than the ISP. ISPs pose a much greater threat to privacy than other online entities and they even pose a greater threat than offline institutions as well, including doctors, psy-

chiatrists, and lawyers." Greater, even, than Google.

Internet-savvy users are fully aware of this, of course, but most haven't had major concerns about all that sensitive data they're pushing through the tubes. ISPs have generally been solid on privacy, as Ohm concedes, and they've lacked the technical means to really invade that privacy, anyway. So why all this talk of a privacy apocalypse that will see blood raining from the skies and screams of the damned outside making it tough to keep concentrating on that World of Warcraft session?

The two bulldozers, in Ohm's view, that are remaking the ISP landscape are "deep packet inspection gear" and "tremendous commercial pressures." ISPs at last have the technical capacity to monitor huge amounts of user web traffic in realtime, and advertisers like NebuAd and Phorm are (or were) simultaneously offering large cash payments for access to Internet traffic.

Apart from these two major commercial forces, government mandates also lurk in the background. CALEA rules have forced ISPs to install this sort of gear in order to provide full wiretap access to a user's Internet data stream when required by law. And content owners have been leaning on governments around the world, which in turn are leaning on ISPs to do something about the illicit P2P problem. Filtering has been one solution beloved of copyright owners, and ISPs like AT&T have even publicly committed to doing so. And then, of course, there's Comcast.

More at <http://arstechnica.com/news.ars/post/20080907-prof-rails-against-greatest-reduction-of-user-privacy-in-net-history.html>

### Google cuts how long it stores users' personal data

REUTERS

MOUNTAIN VIEW, California - Google Inc has halved the amount of time it stores personal data gathered from its users' Web surfing habits, a move aimed at improving its privacy policies, a company official said.

Google used to store such data for 18 months, but has now trimmed that duration to nine months.

Nicole Wong, Google's deputy general counsel, told a meeting of computer industry privacy experts at Microsoft Corp's Silicon Valley offices that her company planned to "anonymize" the computer addresses of its users more quickly.

"We're significantly shortening our previous 18-month reten-

tion policy to address regulatory concerns and to take another step to improve privacy for our users," Google officials said in a blog post released Monday night.

Peter Cullen, chief privacy strategist for Microsoft Corp, said Google's move was done in response to pressure from European regulators and by industry rivals.

Cullen, who was taking part in panel discussion with Wong, said that until a year-and-a-half ago, Google had kept personally identifiable information about its Web users on company computers for an indefinite amount of time.

Google adopted an 18-month privacy policy only after pressure from the European Union, he said.

Source: <http://www.reuters.com/article/rbssTechMediaTelecomNews/idUSN0847077420080909>

## NEW REPORTS AND PAPERS

### How Economic News Moves Markets

*FEDERAL RESERVE BANK OF NEW YORK*

The Federal Reserve Bank of New York today released *How Economic News Moves Markets*, the latest article in its series *Current Issues in Economics and Finance*.

Investigating how the issuance of new economic data influences asset prices in the stock, bond and foreign exchange markets, authors Leonardo Bartolini, Linda Goldberg and Adam Sacarny conclude that only a few announcements—the nonfarm payroll numbers, the GDP advance release and a private sector manufacturing report—have significant and persistent effects. Most of the other data releases examined, the authors find, generate only transitory or erratic responses.

Adopting the methodology used in other recent studies, Bartolini, Goldberg and Sacarny use high-frequency data on asset prices to track the effects of news about thirteen heavily watched economic indicators over the 1998-2007 period. Specifically, they seek to assess how stock prices, bond yields and exchange rates react to the “surprise component” in economic announcements—that is, the difference between the actual value announced for a particular indicator and the

value that market participants had expected. The authors observe these reactions over two time horizons: within thirty minutes of the announcement and through 4 p.m. on the day of the announcement.

The analysis yields a number of lessons on the scale and persistence of asset price responses. In addition to identifying the announcements that have significant and longer-lasting effects, the authors determine that bond yields show the strongest response to economic announcements while stock prices show the weakest. As for the direction of these effects, news of higher-than-expected growth and inflation generally leads to a rise in bond yields and the exchange value of the dollar. While the size of news effects on asset prices tends to be consistent throughout the day, the immediate impact can be measured more precisely than the full-day impact.

Leonardo Bartolini is a senior vice president, Linda Goldberg a vice president, and Adam Sacarny an assistant economist in the International Research Function of the Bank’s Research and Statistics Group.

More at <http://www.newyorkfed.org/newsevents/news/research/2008/rp080908.html>

### How Can Decision Making Be Improved?

*HARVARD BUSINESS SCHOOL*

#### Executive Summary:

While scholars can describe how people make decisions, and can envision how much better decision-making could be, they still have little understanding of how to help people overcome blind spots and behave optimally. Chugh, Milkman, and Bazerman organize the scattered knowledge that judgment and decision-making scholars have amassed over several decades about how to reduce biased decision-making. Their analysis of the existing literature on improvement strategies is designed to highlight the most promising avenues for future research. Key concepts include:

- People put great trust in their intuition. The past 50 years of decision-making research challenges that trust.
- A key task for psychologists is to identify how and in what decision-making situations people should try to move from intuitive, emotional thinking to more deliberative, logical thinking.
- The more that researchers understand the potentially harmful effects of some biased decision-making, the more

important it is to have empirically tested strategies for reaching better decisions.

#### Abstract

The optimal moment to address the question of how to improve human decision making has arrived. Thanks to fifty years of research by judgment and decision making scholars, psychologists have developed a detailed picture of the ways in which human judgment is bounded. This paper argues that the time has come to focus attention on the search for strategies that will improve bounded judgment because decision making errors are costly and are growing more costly, decision makers are receptive, and academic insights are sure to follow from research on improvement. In addition to calling for research on improvement strategies, this paper organizes the existing literature pertaining to improvement strategies, highlighting promising directions for future research.

Daniel Kahneman, Amos Tversky, and others have clarified the specific ways in which decision makers are likely to be biased. As a result, we can now describe how people make decisions with astonishing detail and reliability. Furthermore, thanks to the normative models of economic theory, we have a clear vision of how much better decision making could be.

More at <http://hbswk.hbs.edu/item/5976.html>

## NEW REPORTS AND PAPERS - II

### Terrorism and the Proportionality of Internet Surveillance

BY IAN BROWN, DOUWE KORFF,  
*EUROPEAN JOURNAL OF CRIMINOLOGY*

#### Abstract:

As the Internet has become a mainstream communications mechanism, law enforcement and intelligence agencies have developed new surveillance capabilities and been given new legal powers to monitor its users. These capabilities have been particularly targeted toward terrorism suspects and organisations, which have been observed to use the Internet for communication, propaganda, research, planning, publicity, fundraising and creating a distributed sense of community. Policing has become increasingly pre-emptive, with a range of activities criminalised as "supporting" or "apologising for" terrorism. The privacy and non-discrimination rights that are core to the European legal framework are being challenged by the increased surveillance and profiling of terrorism suspects. We argue that their disproportionate nature is problematic for democracy and the rule of law, and will lead to constitutional challenges in states such as Germany.

#### Introduction

Over the last 15 years the Internet has developed from a specialist network of academic researchers into a mainstream

communications mechanism. Around 60% of the UK population are now regular Internet users, most commonly for e-mail and web browsing (Dutton and Helsper 2007).

As might be expected of any such widespread technology, law enforcement agencies have paid increasing attention to the use of the Internet for criminal purposes, especially by terrorism suspects. Terrorist groups such as Hezbollah have been observed to use the Internet for communication, propaganda, research, planning, publicity, fundraising and creating a distributed sense of community. E-mail and web discussion forums have been used to plan operations, while websites are commonly used to bypass media editorial controls and communicate directly with groups' supporters and potential recruits (Bird 2006; Labi 2006).

In response to this activity policing and intelligence agencies have developed new capabilities and successfully lobbied for new legal powers to put Internet users under surveillance. These have included requirements for Internet Service Providers to facilitate wiretaps and to store information about their customers' communications and Web browsing activities (Brown and Korff 2004; Schjolberg 2007). However, these new powers have caused significant concern that the private lives of Internet users with no connection to terrorism or serious crime are being disproportionately invaded, and that in the words of UK Information Commissioner Richard Thomas we are "sleepwalking into a surveillance society" (Ford 2004).

More at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1261194](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261194)

### The Rise and Fall of Invasive ISP Surveillance

BY PAUL OHM, *UNIVERSITY OF COLORADO*

#### Abstract:

Nothing in society poses as grave a threat to privacy as the Internet Service Provider (ISP). ISPs carry their users' conversations, secrets, relationships, acts, and omissions. Until the very recent past, they had left most of these alone because they had lacked the tools to spy invasively, but with recent advances in eavesdropping technology, they can now spy on people in unprecedented ways. Meanwhile, advertisers and copyright owners have been tempting them to put their users' secrets up for sale, and judging from a recent flurry of reports, ISPs are giving in to the temptation and experimenting with new forms of spying. This is only the leading edge of a coming storm of unprecedented and invasive ISP surveillance.

This Article proposes an innovative new theory of communications privacy to help policymakers strike the proper balance between user privacy and ISP need. We cannot simply ban aggressive monitoring, because ISPs have legitimate reasons for

scrutinizing communications on an Internet teeming with threats. Using this new theory, policymakers will be able to distinguish between an ISP's legitimate needs and mere desires.

In addition, this Article injects privacy into the network neutrality debate - a debate about who gets to control innovation on the Internet. Despite the thousands of pages that have already been written about the topic, nobody has recognized that we already enjoy mandatory network neutrality in the form of expansive wiretapping laws. The recognition of this idea will flip the status quo and reinvigorate a stagnant debate by introducing privacy and personal autonomy into a discussion that has only ever been about economics and innovation.

#### Introduction

Internet Service Providers (ISPs) I have the power to obliterate privacy online. Everything we say, hear, read, and do on the Internet passes first through their computers. If ISPs wanted, they could store it all, compiling a perfect transcript of our online lives.

More at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1261344](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261344)

## NEW REPORTS AND PAPERS - III

### The Influence of Personality Traits and Information Privacy Concerns on Behavioral Intentions

BY MELINDA L KORZAAN, KATHERINE T BOSWELL, *REDORBIT*

#### Abstract

This study incorporates the Big Five personality traits into a theoretical model that explains and predicts individuals' concerns for information privacy, computer anxiety, and individual behavioral intentions. Data was gathered via a survey, which was completed by 230 undergraduate college students, and analysis was conducted utilizing structural equation modeling. Agreeableness was found to have a significant influence on individual concerns for information privacy while neuroticism was found to have a significant influence on computer anxiety. In addition, intellect exerted a significant influence on both computer anxiety and behavioral intentions. Key insights for theory and practice are presented.

#### Introduction

Businesses are increasingly dependent upon technology to enhance their on-going operations as well as to recognize and capitalize on potential opportunities. However, concerns have arisen regarding some of the applications for which this technology is being utilized. For the last couple of decades, especial-

ly in the aftermath of 9/11, privacy issues have been in the forefront of individuals' concerns. Various privacy acts have been passed to help protect individual's personal information and privacy policies have become an accepted practice in most industries. The shift toward e-commerce has exacerbated the concern over information privacy and has spawned a greater awareness by the public of the potential risks that are associated with unsafe information practices. Awareness is increasing regarding the risk associated with providing personal data using technology. These risks range from phishing scams to identity theft. All in all, society is becoming more hesitant about providing complete and accurate personal data.

A CBS news report, states that 2/3 of Americans think the US government should be doing more to regulate the collection of personal information. This report goes on to say that 52% of the respondents believe their privacy rights are in serious jeopardy and 30% believe privacy rights are already non-existent. In addition, the report states that even after explaining why businesses collect personal information (both positive and negative), 83% of individuals surveyed still had an overall negative reaction to such business practices. Other reports have stated that consumers are becoming more diligent about protecting their own privacy by using privacy tools available and withholding more sensitive information.

More at [http://www.redorbit.com/news/technology/1548286/the\\_influence\\_of\\_personality\\_traits\\_and\\_information\\_privacy\\_concerns\\_on/](http://www.redorbit.com/news/technology/1548286/the_influence_of_personality_traits_and_information_privacy_concerns_on/)

### Healthcare IT - "It's A Sleeping Giant"

*HIMSS Global Enterprise Task Force (GEFT) investigates implementation of electronic health records (EHRs) in 15 countries around the world*

*HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY*

**CHICAGO** (Sept. 5, 2008) – Recognizing common threads that affect all EHR implementations in 15 countries, the Global Enterprise Task Force of the Healthcare Information and Management Systems Society (HIMSS) has released "Electronic Health Records: A Global Perspective." The extensive study reviewed healthcare IT progress in Europe, Asia Pacific, Middle East and North America.

The 16-member task force looked at various EHR components within each country, including, security, quality, financing sources and barriers to adoption. Amid many variations, four common factors emerged that affect implementation of the electronic

health record throughout the world. They are:

- Funding
- Governance
- Standardization and interoperability
- Communication

"This comprehensive report provides actionable lessons learned from each of the countries we reviewed. Despite the local differences in the logistics of EHR implementation, we found that all of the countries believed in the benefits of health IT and introduced this technology into their respective health systems," said Steve Arnold, MD, MS, MBA, CPE, chair of the task force and president/CEO, Healthcare Consultants International, Lagrangeville, NY. Walter W. Wieners, FHIMSS, co-chaired the task force and is managing principal, Walter W. Wieners Consulting, Sausalito, Calif.

The 119-page report presents findings on EHR implementation by country in five categories. Each chapter features an overview of the country's electronic health record status followed by a review of achievements, barriers and recommendations in the different areas.

More at <http://www.himss.org/ASP/ContentRedirector.asp?ContentId=68380&type=HIMSSNewsItem>

## NEW REPORTS AND PAPERS - IV

### The Shape of Things to Come

BY TONY BUNYAN, *STATEWATCH*

#### Introduction

This analysis looks at the ideology in the Future group report, Freedom, Security and Privacy - the area of European Home Affairs. The EU is currently developing a new five year strategy for justice and home affairs and security policy for 2009-2014. The proposals set out by the shadowy 'Future Group' include a range of extremely controversial measures including techniques and technologies of surveillance and enhanced cooperation with the United States.

This examines the proposals of the Future Group and their relation to existing and planned EU policies. It shows how European governments and EU policy-makers are pursuing unfettered powers to access and gather masses of personal data on the everyday life of everyone – on the grounds that we can all be safe and secure from perceived "threats".

The Council of the European Union's "Future Group" presented its final report at the Justice and Home Affairs Council's July 2008 meeting. This will lead to a new justice and home affairs programme for 2010-2014, following the "Tampere" programme (1999-2004) and the "Hague" programme 2005-2009. The final programme will be proposed by the European Commission, then amended and adopted by the Council. It will set out a detailed programme for both

new measures and practices for the five-year period.

The "Timetable" indicates that the new five year plan will be adopted under the Swedish Council Presidency in the second half of 2009 – the "Stockholm programme" maybe.<sup>3</sup> The final report is intended to be the basis of a proposal from the European Commission and unlike the processes for the adoption of the Tampere and Hague programmes it also suggests that the European Parliament will be consulted - but, as usual, the Council of the European Union (the 27 governments) will have the final say on its content.

The group was set up in January 2007 - Ministers had agreed to a German Presidency proposal at the Informal JHA meeting in Dresden on 14-16 January 2007 and later "in the margins" of the JHA Council on 14 February 2007.<sup>4</sup> Its final report is from the "Informal High Level Advisory Group on the Future of European Home Affairs Policy" and is entitled: Freedom, Security and Privacy - European Home Affairs in an open world. A separate report was also published on Justice.<sup>5</sup> The Tampere and Hague programmes were concerned with both home affairs and justice so this separation is unusual but deliberate - in many member states the Justice Ministries are often perceived as being more "liberal" as they cover peoples' rights in the criminal justice system whereas Interior Ministries are more concerned with the agencies that exercise coercive powers over citizens and migrants.

More at <http://www.statewatch.org/analyses/the-shape-of-things-to-come.pdf>

### Wasted Lessons of 9/11: How the Bush Administration Has Ignored the Law and Squandered its Opportunities to Make our Country Safer

*U.S. HOUSE OF REPRESENTATIVES*

#### Executive Summary

On September 11, 2001, this country suffered the most devastating terrorist attacks ever experienced on our soil. The series of coordinated attacks, perpetrated by 19 hijackers affiliated with al Qaida, killed 3,000 people, inflicted hundreds of millions of dollars of economic damage, brought commercial aviation to a standstill, and opened the eyes of the American people to the threat of terrorism as never before.

To establish how the perpetrators were able to execute their deadly plot, Congress chartered the independent, bipartisan National Commission on Terrorist Attacks Upon the United States (9/11 Commission). In addition to providing a full account of the circumstances surrounding the attacks, Congress directed the 9/11 Commission to develop recommendations

for corrective measures that could be taken to prevent future acts of terrorism.<sup>1</sup> On July 22, 2004, the 9/11 Commission issued its final report, which included 41 wide-ranging recommendations to help prevent future terrorist attacks. Many of these proposals were put in place in 2004 with the passage of the Intelligence Reform and Terrorism Prevention Act<sup>2</sup>, which brought about the most significant reorganization of the intelligence community since 1947. Among the key provisions of that law was the establishment of a Director of National Intelligence to oversee the intelligence community and the creation of a National Counterterrorism Center to analyze domestic and international threats, share that information, and integrate activities to ensure unity of effort against terrorism.

Yet, a year after it was issued, the lead authors of the 9/11 Commission Report, Governor Thomas H. Kean and Representative Lee H. Hamilton, asked "[a]s a result of these and other reforms, are we safe? We are safer – no terrorist attacks have occurred inside the United States since 9/11 – but we are not as safe as we need to be. . . . [T]here is so much more to be done. . . ."

More at <http://homeland.house.gov/SiteDocuments/20080909151532-76784.pdf>

## NEW REPORTS AND PAPERS - V

### Searching in Space and Minds: Research Suggests Underlying Link

NEWSWISE

New research from Indiana University has found evidence that how we look for things, such as our car keys or umbrella, could be related to how we search for more abstract needs, such as words in memory or solutions to problems.

"Common underlying search mechanisms may exist that drive our behavior in many different domains," said IU cognitive scientist Peter Todd. "If how people search in space is similar to how they search in their minds, it's a very exciting prospect to try to find the deep, underlying roots of human behavior that may be common to varied domains."

Lead author Thomas Hills worked with Todd and fellow IU cognitive scientist Robert Goldstone in designing experiments to explore the search processes their study participants used in both spatial and abstract settings. The studies revolved around two search modes -- exploitation, where seekers stay with a place or task until they have gotten appreciable benefit from it, and exploration, where seekers move quickly from one place or one task to another, looking for a new set of resources to exploit. They then examined whether an initial search, in this case for resources in space, primed the mode used in the subsequent, more abstract search.

"We asked the question -- are the same mechanisms that let simpler organisms search in space for food related to how we search for things in our mind, for concepts or ideas," Todd said. "Our conclusion is that they seem to be linked at some level, which is what our priming experiment suggests."

Some people might be more inclined to one search mode or the other, having a lesser ability to focus on a given task or difficulty letting go of an idea. An extreme form of the exploratory cognitive style would be someone with attention deficit hyperactivity disorder. An extreme form of the exploitive cognitive style would be someone with obsessive compulsive disorder.

These new findings, published in the latest issue of Psychological Science, have possible implications related to other recent work on brain chemistry and cognitive disorders. Exploratory foraging -- actual or abstract -- appears to be linked to decreases in the brain chemical dopamine. Many problems related to attention -- including ADHD, drug addiction, some forms of autism and schizophrenia -- have been linked to such a dopamine deficit. The authors suggest that computer foraging, such as that used for their experiments, could reveal individual differences in underlying cognitive search style, and could even be used to manipulate that style. If that were possible, it could perhaps lead to therapies for such cognitive disorders.

More at <http://www.newswise.com/articles/view/544176/>

### The NPD Group: Wired Baby Boomers Going Digital, Visiting Social Networks and Watching Videos on the Web

*"Entertainment Trends in America" report reveals boomers are key demographic segment for digital products and marketing; Baby boomers who stream video 15 percent more likely to buy a CD, DVD, or movie tickets*

CENTRE DAILY

PORT WASHINGTON, N.Y. — According to The NPD Group, a leading market research company, online activities once mainly popular with teens and young adults, are now enjoying active participation by baby boomers, too. Recent consumer surveys of U.S. consumers show that 61 percent of baby boomer Internet users (age 44 to 61) had visited sites that offer streaming or downloadable video (e.g., YouTube and TV network Web sites), while 41 percent had visited social networks

(e.g., Linked-In, Facebook, and MySpace).

"There's an ongoing misperception that certain Web activities are the exclusive domain of young people," said Russ Crupnick, entertainment industry analyst for The NPD Group. "That misperception could cost the entertainment industry, in terms of lost opportunities to target valuable consumers."

NPD's "Entertainment Trends in America" tracking study reveals that more than half of all Web users (57 percent) visited a social networking site in past three months. Although young Web users (13- to 34-year-olds) are significantly more likely to visit social networking sites -- and to visit them more often -- baby boomers who visited social networking Web sites did so an average of 8 times over the previous three months.

When it comes to the Web's effect on sales of traditional entertainment content, NPD found that baby boomers who engage in activities, like social networking or video streaming, are also more likely to buy DVDs, CDs and go out to the movies. NPD noted that, on average, baby boomers who stream video are also 15 percent more likely than their non-streaming counterparts to buy a CD, DVD, or movie tickets.

More at <http://www.centredaily.com/business/technology/story/827822.html>

## NEW REPORTS AND PAPERS - VI

### New Report: Pilot Test Shows Patient-Centered Medical Homes for Primary Care Can Reduce Hospital Admissions and Total Medical Costs

*THE COMMONWEALTH FUND*

**New York, NY, September 10, 2008**—Geisinger Health System in Pennsylvania reduced hospital admissions by 20 percent and saved 7 percent in total medical costs by providing a patient-centered medical home (PCMH) model of care—including around-the-clock access to primary and specialty care, and physician and patient access to electronic health records (EHRs)—according to first-year results from pilot-test sites. The findings, released in the September/October issue of *Health Affairs*, provide the first evidence that the PCMH model can improve quality of care and reduce health care costs. The article also describes Geisinger Health System's efforts to redesign its care delivery infrastructure and to create incentives aligned to enhanced health care value.

"These findings point to the potential for innovative and integrated delivery systems to improve health care quality," said Glenn Steele, M.D. CEO of the Geisinger Health System. "When hospitals, specialists, and primary care practices work together, with the support of quality improvement and innovation units and information technology systems, they gain the efficiencies and focus needed to deliver high quality care."

"This is the direction in which we need to move our fragmented, broken health care system," said Commonwealth Fund President Karen Davis, who is a board member of the Geisinger

Health System and co-authored the article, "Continuous Innovation in Health Care: Implications of the Geisinger Experience," with Geisinger's Chief Technology and Innovation Officer Ronald Paulus, M.D., and President and CEO Glenn Steele, M.D.

The authors point to lessons from the Geisinger success that can inform national policies aimed at improving value in health care, including:

- By offering new payment schemes and incentives, such as acute episode global fees and payments for patient-centered medical homes, commercial insurers, Medicaid, and Medicare could encourage a broader array of providers to implement these improvements.
- Electronic health records are necessary but not sufficient to improve health care delivery and value; health care delivery systems need to be organized in ways that can take full advantage of the benefits of EHRs.
- Collaboration by public and private payers to align incentives which improve health care can help replicate these successes.

Geisinger's innovations show considerable promise for improving quality and enhancing value. For their best practices and care models to spread more broadly, health policies to align payment incentives, encourage greater organization of care delivery, and adoption of modern information technology are needed.

More at [http://www.commonwealthfund.org/newsroom/newsroom\\_show.htm?doc\\_id=704661](http://www.commonwealthfund.org/newsroom/newsroom_show.htm?doc_id=704661)

### Online Health Information Category Grows at Rate Four Times Faster Than Total Internet

*Category Up 21 Percent in Past Year  
WebMD Health Ranks as Top Publisher  
of Display Ads*

*PRNEWSWIRE-FIRSTCALL VIA COMTEX*

**RESTON, Va., Sept 09, 2008** - comScore, Inc. , a leader in measuring the digital world, today released results of a study showing that the health information site category has grown 21 percent during the past year -- more than four times the growth rate of the total U.S. Internet population.

While WebMD Health continues to lead the category with 17.3 million visitors in July (up 3 percent versus year ago),

three other health networks boosted the overall growth of the category, each attracting more than ten million visitors: Everyday Health with 14.7 million (up 63 percent), Revolution Health Network with 11.3 million visitors (up 182 percent), and AOL Health with 11.1 million (up 88 percent). While Everyday Health and Revolution Health Network both achieved significant organic growth on their core Web sites, their recent partnerships with several smaller health sites, as well as some strategic acquisitions, have also contributed to their respective gains.

"Improved site functionality, increased content personalization, and overall consumer acceptance of the Internet as a source for health information have helped to breathe new life into the health information category," said John Mangano, senior director, comScore Pharmaceutical Marketing Solutions.

More at <http://www.marketwatch.com/news/story/online-health-information-category-grows/story.aspx?guid={56CE38BD-3AD4-41B6-B86B-E086C61EDAD0}&dist=hppr>

## POINTS OF VIEW

### Community cleverness required *Researchers need to adapt their institutions and practices in response to torrents of new data — and need to complement smart science with smart searching.*

NATURE

The Internet search firm Google was incorporated just 10 years ago this week. Going from a collection of donated servers housed under a desk to a global network of dedicated data centres processing information by the petabyte, Google's growth mirrors that of the production and exploration of data in research. All of which makes this an apt moment for this special issue of Nature, which examines what big data sets mean for contemporary science.

'Big', of course, is a moving target. The portability of the tens of gigabytes we carry around on USB sticks would have seemed like fantasy a few years ago. But beyond a certain point, as an increasing number of research disciplines are discovering, the vast amounts of data are presenting fresh challenges that urgently need to be addressed.

The issue is partly a matter of the sheer scale of today's data sets. Managing this torrent of bits has forced more and more fields to move to industrial-scale data centres and cutting-edge

networking technology (see page 16). But the data sets are also becoming increasingly complex. As researchers study the inner workings of the cell, for example, they now gather data on genomic sequences, protein sequences, protein structure and function, bimolecular interactions, signalling and metabolic pathways, regulatory motifs — on and on. No wonder even the smartest scientists turn with relief to advanced data-mining tools, online community collaborations (see page 22) and sophisticated visualization techniques (see page 30).

Sudden influxes of data have transformed researchers' understanding of nature before — even back in the days when 'computer' was still a job description (see page 36). Unfortunately, the institutions and culture of science remain rooted in that pre-electronic era. Taking full advantage of electronic data will require a great deal of additional infrastructure, both technical and cultural (see pages 8, 28 and 47).

The lack of standards, for instance, confounds many a researcher seeking to harness the diversity of knowledge now available on any chosen topic. All credit, then, to those in the vanguard of interoperability. In biology, for example, the Gene Ontology Consortium has spent the past decade devising consistent descriptions of gene products in different databases. Meanwhile, the Mouse Genome Informatics resource is a good demonstrator of complexity's challenges and solutions.

More at <http://www.nature.com/nature/journal/v455/n7209/full/455001a.html>

### Information Sharing: Vital Building Block Toward a Safer and More Secure Nation

U.S. DEPARTMENT OF HOMELAND SECURITY

We all know how catastrophic the results can be when the right people do not get the right information at the right time. That is why we have made information sharing a national priority, and here at the Department of Homeland Security, a critical part of our mission.

Virtually everyone at DHS has a role in information sharing, which is an essential weapon against threats to the homeland. As those who want to do harm to the nation become more sophisticated, we, too, must be more creative and develop innovative ways to thwart potential attacks. We must continue working to develop coherent policies, create effective governance structures and break down any barriers that prevent us from building sustainable networks and relationships that will secure the nation -- not only now, but in the years to come.

The recently released DHS Information Sharing Strategy exemplifies the Department's commitment to doing exactly that. A

first-of-its-kind document for DHS, the strategy provides direction and guidance for all of the Department's information-sharing initiatives. It describes how we can transform DHS into an organization that promotes an environment where information is shared in a strategic, efficient manner.

The Strategy is based on a set of five guiding principles:

- Fostering information sharing is a core Department mission.
- The Department must use the established governance structure to make decisions regarding information-sharing issues.
- The Department must commit sufficient resources to information sharing.
- The Department must measure progress toward information sharing goals.
- The Department must maintain information and data security and protect privacy and civil liberties.

More at <http://www.dhs.gov/journal/leadership/2008/09/information-sharing-vital-building.html>

## POINTS OF VIEW - II

### The 'surveillance society' has led to many terrorists being imprisoned

BY PETER CLARKE, *TIMES ONLINE*

So was there or was there not a plot to bring down airliners? I know what I think. The jury agreed that some of those on trial wanted to commit murder, but couldn't agree, despite strong evidence, that the targets were airliners.

They have not rejected the possibility, and while the lawyers pick the bones out of the messy end to this trial we can still be satisfied with what the "surveillance society" has achieved. Many innocent people, targets of a group of homicidal terrorists, are safely at work, at home or on holiday with their families.

But the terrorists didn't end up in prison by accident. They didn't suffer a pang of conscience, give themselves up to the police and throw themselves on the mercy of the courts. They were hunted down by the most sophisticated counter-terrorist bodies in the world, and convicted by one of the oldest judicial systems.

On the evening of August 9, 2006, I was told that a man connected to the British terrorists had been arrested in Pakistan. This was not good news. We were at a critical point in building our case against them. If they got to hear that he had been arrested they might destroy evidence and scatter to the four winds. More worrying still, if they were tipped off to the arrest they might panic and mount a desperate attack.

### Why All the Data Breaches? Businesses Just Don't Care

BY BEN WORTHEN, *WALL STREET JOURNAL*

U.S. businesses reached an ignominious milestone in August, when the number of data breaches disclosed publicly for the first eight months of 2008 already surpassed the total number of disclosed breaches for all of last year.

There were 449 publicly disclosed security breaches as of Aug. 22, compared with a 446 total in 2007, according to Identity Theft Resource Center, a San Diego nonprofit organization for victims of identity theft. The reasons why businesses struggle keeping customer or employee data secure are many: Cyber criminals are adopting more sophisticated techniques for breaking into businesses; businesses are creating, storing, and sharing more data than ever before; and employees don't understand the value of the data that they work with or the myriad ways the data could fall into the wrong hands.

All of these make tech security difficult—but not impossible. The real reason that data breaches are on the rise is that businesses don't have a real incentive to invest more than the min-

imum required in security, says Bruce Schneier, chief security technology officer at BT Group.

At Scotland Yard we decided, in a matter of minutes, that Operation Overt had to be brought to an end and all 20 suspects arrested immediately. Detectives rushed to the Yard from all quarters, were briefed and sent to make their arrests. In the operations room, as the night wore on, the number of red dots against suspects' names, used to signify they had been arrested, steadily grew. By morning, all were in the cells.

The convictions secured yesterday are another important landmark in a series of terrorist cases stretching back to 2004. The common denominator in each is Pakistan, with British terrorists travelling there for training and tasking. Dig deep enough and you will find connections between them all: some clear, some opaque and some assumed by virtue of coincidence of travel patterns. For instance, it is a fact that some members of several of these plots were in Pakistan at the same time in 2004.

Are there more plots directed at the UK from this source? I would be amazed if there were not. Al-Qaeda have proved to be incredibly resilient. Time and again they have been attacked, suffered losses, both on the battlefield and in the courtroom, and yet still they keep coming. Now is not the time to take off the pressure.

More at <http://www.timesonline.co.uk/tol/news/uk/crime/article47-10870.ece>

imum required in security, says Bruce Schneier, chief security technology officer at BT Group.

"For the most part a company doesn't lose its data, they lose your data," Schneier tells the Business Technology Blog. Consequently, the entity responsible for the breach isn't the party that is harmed by it. Victims are upset, but they are more likely to learn about the fraud that is committed in their name—not the breach where a criminal obtained the data. They are often powerless to punish the business that exposed the record because they can't link the fraud to a cause, says Schneier.

At least 44 states have laws that require businesses to disclose data breaches. But a recent study by researchers at Carnegie Mellon University found no evidence that these laws actually reduce the incidents. There are potential loopholes: Sometimes only businesses in certain industries must disclose a breach; or the breach may only have to be disclosed if a business suspects that the information will be used to commit fraud. Also, aside from potentially negative publicity, businesses are rarely penalized for a breach as long as it is disclosed.

More at <http://blogs.wsj.com/biztech/2008/09/09/why-all-the-data-breaches-businesses-just-dont-care/>

## POINTS OF VIEW - III

### Secrecy Report Card

#### *OPEN THE GOVERNMENT*

##### Executive Summary

OpenTheGovernment.org's fifth annual report, Secrecy Report Card 2008, shows both a continued expansion of government secrecy across a broad array of agencies and actions and some movement toward more openness and accountability, particularly in the Congress.

The public has a right to know what its government is doing to preserve health, safety, and the public weal. Information created by or for the federal government belongs to the American public and should be open (except in strictly limited and specified contexts). The administration of President George W. Bush has over its seven and one half years to date exercised unprecedented levels not only of restriction of access to information about federal government's policies and decisions, but also of suppression of discussion of those policies and their underpinnings and sources. It continues to refuse to be held accountable to the public through the oversight responsibilities of Congress. We have been made less secure as a result and the open society on which we pride ourselves has been undermined and will take hard work to repair.

##### Highlights

- The government spent \$195 maintaining the secrets already on the books for every one dollar the government spent declassifying documents in 2007, a 5% increase in one year. At the same time, fewer pages were declassified than in 2006, even though the government spent the same amount of money on declassification. The intelligence agencies, which account for a large segment of the declassification numbers, are excluded from the total reported figures.
- In 2007, the number of original classification decisions increased slightly to 233,639, after dropping two years in a row. The numbers remain significantly higher than before 2001. The number of derivative classifications also increased from 20,324,450 in 2006 to 22,868,618 in 2007 — an increase of almost 13%.
- The total cost of FOIA implementation in 2007 across the government increased 16%. But a 2008 study by the Coalition of Journalists for Open Government (CJOG) revealed that, in 2007, FOIA spending at the 25 agencies it examined fell by \$7 million to \$233.8 million and the agencies put 209 fewer people to work processing FOIA requests.
- Almost 22 million FOIA requests were received in 2007, an increase of almost 2% over last year. Agencies are not, however, taking advantage of significant opportunities to reduce their backlogs: the 25 departments and agencies that handle the bulk of the third-party information requests received the fewest requests since reporting began in 1998 — 63,000 fewer than 2006 — but they processed only 2,100 more requests than they did in 2006 (when the backlog soared to a record 39%).
- In the fiscal year ending September 30, 2007, the United States obtained over \$2 billion in settlements and judgments concerning fraud on the United States, \$1.45 billion as a result of whistleblower qui tam suits. However, DOJ faces an ever-growing backlog of over 900 cases. Since 1986, whistleblowers helped the federal government recover over \$20 billion according to the latest figures from the U.S. Department of Justice.
- On average since 2000, non-competed contract funding makes up more than 25 percent of all awards. In FY 2007, 26.15 percent (\$114.1 billion) of federal contract funding was given out without any competition; another 5 percent (\$22.9 billion) was awarded without competition because of specific requirements. In 2000, 45 percent of contract dollars were awarded under full and open competition; by 2007, only 33 percent followed such open procedures — a drop of almost 25%. CRECY REPORT CARD 2008 • 4
- With 2,371 secret surveillance orders approved in 2007, federal surveillance activity under the jurisdiction of the secretive Foreign Intelligence Surveillance Court has risen for the 9th year in a row — more than doubling since 2000.
- In 2007, agencies received 7,827 new initial requests for Mandatory Declassification Review (MDR), of which 88% (6,881) were processed, resulting in the declassification of information in 431,371 pages (93%): 75% (347,338) in full; 18% (84,033) in part. Seven percent (30,125 pages) remained classified in their entirety after review. A sizeable backlog of initial requests is carried forward each year, however. For 2007, almost 5,000 initial requests — 42% — were carried over into 2008.

More at <http://www.openthegovernment.org/otg/SecrecyReportCard08.pdf>

## INTERNET GOVERNANCE

### Countries Collaborate To Counter Cybercrime

*The International Multilateral Partnership Against Cyber-Terrorism (IMPACT) has been launched to bring together the global community to prevent and counter cyberthreats. Membership in the organization is open to all countries, so developing nations can take advantage of existing expertise, and larger ones can help stop attacks.*

BY RITA BOLAND, *SCI-TECH TODAY*

It's a small world after all. As the Internet continues to connect peoples across the globe, individuals and groups drawn to destruction find new ways to wreak havoc on communications Relevant Products/Services and services. Now, government leaders are coming together with each other and the private sector to form a united front and fight back because a vulnerability in any region can wreak havoc globally. A new multilateral federation is combating cyberthreats and cyberterrorism, creating greater security in developing networks and stopping dangers before they spiral out of control.

The International Multilateral Partnership Against Cyber-Terrorism (IMPACT) has been launched to bring together the global community to prevent and counter cyberthreats. Membership in the organization is open to all countries, so developing nations can take advantage of existing expertise, and larger ones can help stop attacks. Certain corporations and research agencies also are invited to participate. IMPACT is modeled on the U.S. Centers for Disease Control and Prevention as a government agency interacting with the private and academic sectors.

IMPACT aims to offer network solutions and ideas not available currently. Members will assess security efforts already underway and who is involved with them to determine what needs to be accomplished to protect the network better. The organization aims to fill the gaps it finds in security and defenses. The importance of protecting networks is not confined to ensuring Web sites and e-mails remain viable. Network security also involves guarding critical infrastructure Relevant Products/Services such as transportation, communications, utilities and public services as well as financial services and other personal information.

IMPACT was launched at the World Cyber security Summit during the World Congress on Information Technology (WCIT)

in May in Kuala Lumpur, Malaysia. Malaysia has invested \$13 million to get the organization underway and part of that funding will build a headquarters in the country. The headquarters will be in a high-tech city where most of the multinational companies operating in Malaysia are located. In addition to using the money to create infrastructure, the funds will jumpstart efforts such as writing mission and vision statements, developing rules of engagement and generating other necessary products. IMPACT also must set a timeline of various benchmarks, incorporating input from member governments.

In addition to the Malaysian funding, another \$1 million was donated to IMPACT by the SANS Institute. Those funds are allocated for a joint project between the institute and IMPACT to increase the cyberdefense capacity of developing countries. IMPACT also has received the endorsement of the International Telecommunication Union (ITU), a United Nations agency, and the Council of Europe is involved with the organization. The council created the Convention on Cybercrime, a treaty signed by various countries.

The thrust behind IMPACT is to become more proactive toward global cyberterrorism and other attacks rather than reactive. Cyberterrorism, as defined by the organization, involves using electronic means to significantly disrupt an economy or pose a significant threat to life and limb. IMPACT also will develop early response systems so threats generated in one region can be eliminated before they spread. The organization wants to establish certain criteria for information assurance, providing a template and other standardizations among different countries for information assurance and cyberterrorism response.

To accomplish its objectives, IMPACT brings together key decision makers who can take substantive action against cyberattacks. The initial meeting at the WCIT was the largest ministerial meeting on cybersecurity, and the goal of creating partnerships among large and small and public and private institutions is a step toward defeating threats in all areas of the network. Almost 30 countries attended. However, certain countries often associated with cyberoperations, including the United States, United Kingdom, China and Russia, were absent. Six non-government organizations also were in attendance.

Through the multilateral effort, smaller countries will be better equipped to protect their portions of the network, and private companies who own part of the network will be in on initiatives from the beginning so they can use research and development funds to create protective tools. "Each country, business and individual has to do their part to secure Cyberspace," Howard Schmidt, a member of the nine-person IMPACT international advisory board, says.

More at [http://www.sci-tech-today.com/story.xhtml?story\\_id=02200295PQGK](http://www.sci-tech-today.com/story.xhtml?story_id=02200295PQGK)

## INTERNET GOVERNANCE - II

### Tech czar might rule policy under Obama

BY DAVID HATCH, *CONGRESS DAILY*

An administration run by Sen. Barack Obama, D-Ill., would likely create a national technology czar with broad authority to develop policy, elevating high-tech issues to the cabinet level in a major recalibration of the government's approach to regulating the communications sector.

The move would have substantial implications for the FCC, an independent agency that could be answerable to a new layer of bureaucracy or bolstered by it, depending on political circumstances.

The plan is being floated by the Democratic presidential nominee's top tech-minded advisers and supporters, including FCC Commissioner Jonathan Adelstein, widely viewed as a contender to run the agency if Obama is elected.

"There's a need for a single source at a White House level to coordinate technology policy across different agencies," Adelstein told CongressDaily late last month after a speech in Denver at the Democratic National Convention.

"They're extremely serious about it," he said of the Obama team, describing the proposal as a "fundamental tenet" of the Democratic nominee's tech agenda.

A chief technology officer would play a lead role in developing national broadband policy, drawing on the expertise of a wide range of departments, including Agriculture, Commerce, Energy, EPA, HHS, HUD and Treasury.

The appointee also might coordinate inter-agency efforts to establish tax certificates designed to boost minority ownership of media properties, oversee spectrum policy and help improve the government's reliance on information technology.

But the idea of a federal tech czar is proving highly controversial, with critics raising concerns about the level of authority he or she would have and increased prospects for turf battles and gridlock that could undermine the overarching goal.

They emphasized that the White House Office of Science and Technology Policy already tackles some responsibilities the CTO would be tasked with.

At a communications forum in July, three of Adelstein's FCC colleagues expressed caution.

Democratic Commissioner Michael Copps said he prefers to make the agency more independent rather than "politicizing"

tech issues at the White House, although he is open to a more narrowly focused national broadband czar.

Republican Commissioner Robert McDowell suggested that each party's view of a CTO hinges on whether it controls the executive branch, while fellow GOP Commissioner Deborah Taylor Tate also worried about harming the commission's independence.

Adelstein dismissed concerns that more bureaucracy and bickering would result. "I really think that there can be better coordination. The FCC alone can't deal with all of these issues," he said, adding that there is a need for a "central focus" on high-tech matters in the White House.

He insisted the proposal is not a byproduct of recent controversy about the commission's approach to regulation. "I think it's really a positive vision for how to improve and deal with some of the inadequacies of the last eight years," he said, referring to the Bush administration, which has been criticized by Democrats for ineffective regulations governing media and telecom companies.

Bill Kennard, who headed the FCC during the Clinton administration and is now a telecom and tech adviser to the Obama campaign, said no determination has been made about which government department, if any, a CTO would join. "We haven't gotten to that level of detail," he said. Kennard is now a managing director with the Carlyle Group, a private equity firm.

Ed Black, president of the Computer and Communications Industry Association, was cautiously supportive, noting during an interview in Denver that a CTO would send a "symbolic message" about Obama's commitment to making technology a bigger priority.

But he cautioned that the new title is not a "silver bullet" for fixing years of what he insists has been neglect. "Such a person can be an advocate and a centralized place to get information," he said.

There have been technology officers at various agencies and departments in the Bush and Clinton administrations but there has never been a government-wide CTO.

Last year, the White House closed its Technology Administration, a division of the Commerce Department, and eliminated the title of undersecretary of technology, a role widely viewed as weak and ineffectual.

The Democratic Party platform calls for creating a CTO "to ensure we use technology to enhance the functioning, transparency and expertise of government," while the GOP platform does not broach the matter.

More at [http://www.nextgov.com/nextgov/ng\\_20080910\\_7809.php](http://www.nextgov.com/nextgov/ng_20080910_7809.php)

**NEXT WEEK**

**SEPTEMBER 15TH, 2008**

9:00 AM - 12:00 NOON. The Information Technology Association of America (ITAA) will host an event titled "A Forum on our National Cyber Security Posture". Michael Chertoff (Secretary of Homeland Security) will speak at 9:00 AM. The price to attend ranges from \$50-\$125. See, <http://www.ita.org/events/event.cfm?EventID=2745>. Location: Ronald Reagan Building and International Trade Center, 1300 Pennsylvania Ave., NW.

**SEPTEMBER 17TH, 2008**

Conference on Health Care Service Innovation. "How can we improve the service of healthcare?" This topic will be examined from a variety of viewpoints including the emerging field of services science, engineering, management, and the field of health services research. Location: Berkeley City Club, 2315 Durant, Berkeley CA. Details at: <http://www.citris-uc.org/shc>

**SEPTEMBER 18TH, 2008**

9:00 AM - 1:15 PM. The Federal Communications Commission (FCC) Public Safety and Homeland Security Bureau will host an event titled "Pandemic Preparedness: Enhancing Communications Response for Health Care and First Responders". Location: FCC, Commission Meeting Room.

**SEPTEMBER 18TH, 2008**

9:00 - 11:00 AM. The House Intelligence Committee (HIC) will hold a closed hearing titled "Cyber Security". See, <http://intelligence.house.gov/EventsItem.aspx?id=379>. Location: Room H-405, Capitol Building.

**SEPTEMBER 18TH - 19TH, 2008**

Conference on Emerging Health Technologies. The specific goals of the conference are: To explore the potential of new personalized health technologies in supporting self-care and personal health; to assess the availability of healthcare knowledge, including comparative effectiveness, needed for effective personalized health; to review commercial opportunities for trans-Atlantic collaborations; to develop recommendations for best practices in personalized health care. Location: Norfolk, VA. Details at: <http://www.phealthusa2008.org/>

**SEPTEMBER 18TH - 19TH, 2008**

Conference on Public Health Informatics – Improving health in low-resource settings through the application of information and communications technologies. To be held at Bell Harbor International Conference Center in Seattle, WA. Details at: <http://www.gpphi.org/>

**September**

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*

**National Healthcare Incentives Institute**

**The Leading Forum on Financial and Non-financial Incentives, Pay for Performance, Gainsharing, Transparency and Payment Reform in American Healthcare**

**October 19 - 21, 2008**

**Marriott Wardman Park Hotel  
Washington, DC**

<http://www.healthcareincentivesinstitute.com/index.html>

America's health system, while the world's leader in many extraordinary complex medical treatments, is expensive and rife with problems of access, cost effectiveness and quality and patient safety. Many critics find perverse tax policy, coverage and payment incentives at the very heart of the challenges facing medical care in the United States. Across the health system healthcare professionals and executives, innovators, entrepreneurs and health reformers are experimenting with innovations in benefit package design, provider payment methodologies, gainsharing and shared ownership arrangements in an effort to reverse perverse incentives to motivate behavior that will improve the nation's health system and to induce practices that will improve access, cost effectiveness and quality and patient safety.

**SITES COMPENDIUM**

[www.arstechnica.com](http://www.arstechnica.com)  
[www.blogs.wsj.com](http://www.blogs.wsj.com)  
[www.centredaily.com](http://www.centredaily.com)  
[www.commonwealthfund.org](http://www.commonwealthfund.org)  
[www.digitalhcp.com](http://www.digitalhcp.com)  
[www.fcw.com](http://www.fcw.com)  
[www.hbswk.hbs.edu](http://www.hbswk.hbs.edu)  
[www.healthcareincentivesinstitute.com](http://www.healthcareincentivesinstitute.com)  
[www.himss.org](http://www.himss.org)  
[www.homeland.house.gov](http://www.homeland.house.gov)  
[www.marketwatch.com](http://www.marketwatch.com)  
[www.modernhealthcare.com](http://www.modernhealthcare.com)  
[www.nature.com](http://www.nature.com)  
[www.newswise.com](http://www.newswise.com)  
[www.newyorkfed.org](http://www.newyorkfed.org)  
[www.nextgov.com](http://www.nextgov.com)  
[www.nytimes.com](http://www.nytimes.com)  
[www.openthegovernment.org](http://www.openthegovernment.org)  
[www.papers.ssrn.com](http://www.papers.ssrn.com)  
[www.pcworld.com](http://www.pcworld.com)  
[www.redorbit.com](http://www.redorbit.com)  
[www.reuters.com](http://www.reuters.com)  
[www.sci-tech-today.com](http://www.sci-tech-today.com)  
[www.statewatch.org](http://www.statewatch.org)  
[www.thenumerati.net](http://www.thenumerati.net)  
[www.timesonline.co.uk](http://www.timesonline.co.uk)



**RESEARCH@MARKLE.ORG**

**Research & Selection: Stefaan Verhulst**  
**Production: swandivedigital**

**Please send your questions, observations and suggestions to [sverhulst@markle.org](mailto:sverhulst@markle.org)**

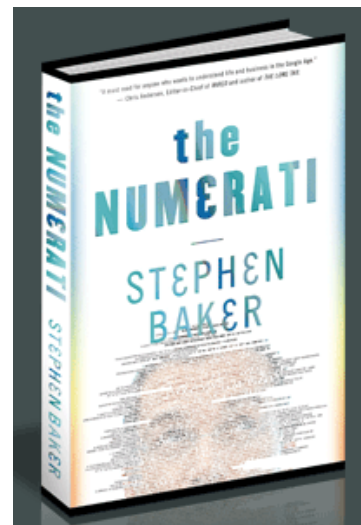
*The views expressed in the Weekly Digest do not necessarily reflect those of the Markle Foundation.*

**BOOK REVIEW****THE NUMERATI**

by Steve Baker

A captivating look at how a global math elite is predicting and altering our behavior -- at work, at the mall, and in bed

Every day we produce loads of data about ourselves simply by living in the modern world: we click web pages, flip channels, drive through automatic toll booths, shop with credit cards, and make cell phone calls. Now, in one of the greatest undertakings of the twenty-first century, a savvy group of mathematicians and computer scientists is beginning to sift through this data to dissect us and map out our next steps. Their goal? To manipulate our behavior -- what we buy, how we vote -- without our even realizing it.



In this tour de force of original reporting and analysis, journalist Stephen Baker provides us with a fascinating guide to the world we're all entering -- and to the people controlling that world. The Numerati have infiltrated every realm of human affairs, profiling us as workers, shoppers, patients, voters, potential terrorists -- and lovers. The implications are vast. Our privacy evaporates. Our bosses can monitor and measure our every move (then reward or punish us). Politicians can find the swing voters among us, by plunking us all into new political groupings with names like "Hearth Keepers" and "Crossing Guards." It can sound scary. But the Numerati can also work on our behalf, diagnosing an illness before we're aware of the symptoms, or even helping us find our soul mate. Surprising, enlightening, and deeply relevant, *The Numerati* shows how a powerful new endeavor -- the mathematical modeling of humanity -- will transform every aspect of our lives.

More at: <http://thenumerati.net/index.cfm?catID=18>