MOBILE DEVICES

Do Tablets Have a Future in Business?

BlackBerry CEO Thorstein Heins predicts that tablets will not prove to be an effective business tool.

"In five years I don't think there'll be a reason to have a tablet anymore; maybe a big screen in your workspace, but not a tablet as such. Tablets themselves are not a good business model," Heins said in a recent interview reported by *Engage.com*.

Some attribute Heins' somewhat controversial remarks to Blackberry's less-than-stellar experience with PlayBook, its version of a tablet. The growth in the use of tablets in the consumer market has clearly seeped into the business market, a trend that some experts believe will continue with the changing demographics of the workforce.

Gartner Inc. predicts that business purchases of tablets will more than triple from 13 million units sold in 2012 to 43 million by 2016. If Gartner is correct, this would, of course, increase the pressure on enterprises to support tablets as business tools.

Yankee Group has expressed a more moderate position. Its research shows a slowing of growth in 2012 and predicts that tablet use in enterprises will flatten in 2013. Yankee Group researchers estimate that 30% of employees will use tablets at work and about 80% of those devices will be employee-owned. Laptops will continue to be the preferred computing method, supported by smartphones for communication. However, the research company does expect tablets to become increasingly popular in retail and other customer-facing positions.

EHR

Pentagon Reassigns EHR Project

It's never good news when the boss takes over your project. Just ask the Pentagon's Military Health System (MHS), which had been tasked with developing a single integrated health records system (iEHR) for the military, in conjunction with the Veterans Affairs Department.

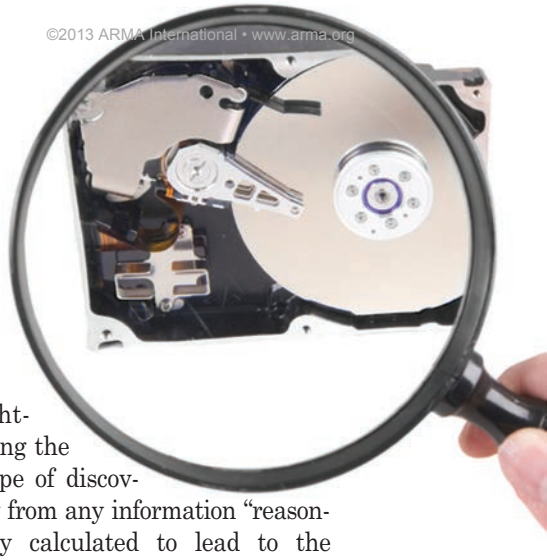
Nextgov reported in April that after having spent $1 billion on building a new system, MHS announced it wanted to take a different course. J. Michael Gilmore, the Pentagon's director of operational test and evaluation, wrote a memo to Deputy Secretary of Defense Ashton Carter stating that MHS preferred to buy commercial health IT software rather than develop systems that are based on open standards as mandated by President Obama in 2009. He added that the department was preparing to distribute a request for proposals.

That's when the boss stepped in.

"I don't think we knew what the hell we were doing," Secretary of Defense Chuck Hagel told a House Appropriations Committee Defense panel in April. That's why Hagel stepped in and took

"personal responsibility" for the iEHR project. According to *Nextgov*, he "deferred" the request for proposals and quietly reassigned the project to Frank Kendall, undersecretary of defense for acquisition, technology, and logistics.

The proposals, which never got past the request-for-information phase, will be in Kendall's hands as Hagel works on the overall plan for iEHR. The plan was expected in June.



E-DISCOVERY

Judges on E-Discovery: Keep It in Perspective

At a recent panel discussion on e-discovery, three influential judges agreed that lawyers must take the lead on decisions of proportionality rather than rely on the judges, who are less familiar with the details of the cases.

The panel, titled "Judges Meet the General Counsel Department," was held at a consortium on litigation, information law, and e-discovery. It focused on the proposed additions to the U.S. Federal Rules of Civil Procedure (FRCP) that concern e-discovery's scope, limitations, and need for cooperation.

According to *Law Technology News*, U.S. District Court Judge Shira Scheindlin was joined by Magistrate Judge James Francis IV who, like Scheindlin, is from the Second District of New York, and Circuit Judge Peter Flynn from the Circuit Court of Cook County in Illinois.

"How am I supposed to conduct proportionality (hearings) – especially right up front?" Scheindlin asked. "It's very difficult to know how to vet things when I know little about the case and have so little time."

Flynn agreed: "Why would anybody ask the judge – who knows the least about the case – to make the decisions?"

Flynn also cautioned against "discovery paranoia – the urge to turn over the next rock, no matter the consequences. Proportionality is an attempt to get people to think about the [possible] costs of turning over the next rock."

The judges also said preservation should be viewed from a business perspective, not as a risk management tool for litigation.

"If you make preservation decisions based on what might be needed in litigation, you are going to save everything, and that's not good for business," Flynn stated.

Francis added that preservation should be just one of the many risk determinations that lawyers make throughout the litigation process.

Scheindlin said the courts may be "moving to staying e-discovery pending a motion to dismiss," thus weeding out cases that cannot proceed.

The advisory committee to the Judicial Conference of the United States proposed significant changes to the FRCP in January. Those changes included limiting the number of production requests and depositions, as well as the amount of time spent on depositions. The committee also proposed tightening the scope of discovery from any information "reasonably calculated to lead to the discovery of admissible evidence," to relevant, non-privileged information that is proportional to the reasonable needs of the case.

Defense attorneys fear limiting discovery will put their clients at a disadvantage. The judges, however, again contend that the key lies with the attorneys talking to each other up front.

E-DISCOVERY

ISO Moves Forward on E-Discovery Standard

A technical committee of the International Organization for Standardization (ISO) has approved moving ahead with a standard for e-discovery, as reported last month in *Law Technology News*. The official title for the standard is ISO/IEC 27050: *Information Technology – Security Techniques – Electronic Discovery*.

Once completed, the new guidance standard will provide an overview of e-discovery and electronically stored information, define terminology, and address the technological and process challenges associated with e-discovery. This will be the first release in what's expected to become a multipart standard that provides requirements as well as guidance.

The new standard will reportedly incorporate elements from the U.S. Seventh Circuit Electronic Discovery Pilot Program, The Sedona Conference®, various state-sponsored best practice guidelines, and contributions from other experts in the field. It is not intended to supersede or contradict local laws and regulations.

Several countries' ISO delegations support the project, including the United States, United Kingdom, China, Mexico, Belgium, Singapore, Norway, Mexico, South Africa, Italy, and the Republic of Korea. Comments and contributions on the working draft will be due by mid-September and processed at the technical committee's meeting in October.

EHR

HHS Puts EHR Vendors on Notice

The U.S. Department of Health and Human Services (HHS) is taking its role seriously when it comes to certifying – or decertifying – electronic health records (EHR) systems. It recently revoked the certification of two systems developed by EHRMagic Inc. after a six-month investigation that stemmed from an anonymous complaint.

An agency spokesperson told Thomson Reuters the certifications were pulled because EHRMagic-Ambulatory and EHRMagic-Inpatient did not meet the "meaningful use" standards. The standards were defined by the Centers for Medicare & Medicaid Services Incentive Programs that govern the use of EHRs and establish the criteria that eligible providers and hospitals must meet to earn incentive payments. The standards are intended to help ensure access to complete and accurate information, which in turn will empower patients to take a more active role in their health management.

There are about 1,800 certified EHR software products available. To qualify for the incentives, healthcare providers must use a certified program and be able to show that the software fulfills the meaningful use requirement.

Henry Ward, an intellectual property and information technology lawyer, told Thomson Reuters that HHS' decision to revoke the certification of the two products "doesn't do a lot in terms of telling the software companies and providers what constitutes meaningful use. [However,] it does provide some context on what doesn't constitute meaningful use." More important, he said, it puts providers and software companies "on notice that the concept of meaningful use has teeth in it."

There are three levels of meaningful use criteria. Stage one (2011-2012) focuses on data capture and sharing; stage two (2014) on advanced clinical processes; and stage three (2016) on improved outcomes. Final rules for the second phase have met some pushback from the industry, which is calling for more time for stage one to ensure systems are working as well as possible and to give more time to ensure integration.

PRIVACY

UK Report: Health Care Too Protective of Patient Data

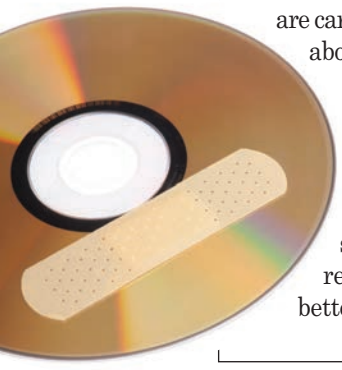
A landmark report on patient information in health and social care in the United Kingdom has raised serious concerns about the balance between protecting the confidentiality of patient data and sharing to improve care, according to *The Guardian*.

"Our conclusion is that the balance isn't right," wrote Dame Fiona Caldicott, who authored the report. "People have become over-concerned about protecting confidentiality."

The UK's former health secretary commissioned Caldicott, a highly respected psychiatrist and psychotherapist, to examine the issue in 2012 following a report from the National Health Service (NHS) Future Forum that identified information governance as an impediment to sharing information, even if sharing would be in the patient's best interest.

Caldicott contends that much of the problem can be attributed to a lack of public education. "While there are professionals who are familiar with the issue of confidentiality, data sharing, and the various systems in place at the moment, we are not sure that the public is given sufficient information," she wrote.

"So I think one of the things is how we can help the public – and of course that is a very varied group of people: some are patients, some are carers, some are healthy but interested, and so on – to know more about what is going on in the new health and social care system."



Caldicott and her team found many instances where IT systems are not linked within hospitals; even fewer are linked between hospitals and other parts of the NHS.

"I think that most NHS patients would be astonished to know that their information doesn't flow around the system," said Health Secretary Jeremy Hunt. He thinks that Caldicott's report provides "the intellectual framework" for approaching better information sharing.

CYBERSECURITY

Privacy vs. Security: A Balancing Act

It's back to the drawing board for the U.S. Congress in its effort to draft cybersecurity legislation that doesn't sacrifice individuals' privacy. Had the most recent bill passed, it was headed for a veto by the White House.

"The president has been clear that the United States urgently needs to modernize our laws and practices relating to cyber security, both for national security and the security of our country's business – but that shouldn't come at the expense of privacy," wrote U.S. Chief Technology Officer Todd Park and Cyber Security Coordinator Michael Daniel, special assistant to the president, in response to an e-petition opposing passage of the Cyber Intelligence Sharing and Protection Act (CISPA).

Balancing privacy and security also emerged as an issue following the bombing at the Boston Marathon in April. The debate centers on the question of whether the bombing could have been prevented if the government and law enforcement could tighten its surveillance measures.

So where should the line be drawn? That's a question that undoubtedly will be argued for some time to come. It is also a global concern. The same debate is taking place in New Zealand, for example.

The New Zealand Herald recently reported that Roy Morgan Research "sounded alarm bells that the government's response to the growing cyber-security threat may undermine liberties." New Zealanders have become increasingly aware of the challenges of balancing security and privacy as a result of the increased use of new technologies over the past couple of years.

"And with the debate raging over proposed legislation to allow spy agencies and the police to conduct cyber surveillance on New Zealand citizens, these are more relevant than ever," said Pip Elliott, chief executive of Roy Morgan Research. She added that the number of citizens who said they were worried about the invasion of their privacy through new technology has increased from 54% to 62% over the past decade; it raised two percentage points in the last two years.

In the United Kingdom, the government recently abandoned its efforts to introduce legislation that would have given security services sweeping powers to monitor Internet activity. Opponents of the legislation heralded the move: "Nick Clegg [deputy prime minister] has made the right decision for our economy, for Internet security, and for our freedom," blogged the campaign group Big Brother Watch.

"Rather than spending billions on another Whitehall IT disaster that tramples over our civil liberties and privacy on an unprecedented scale, we should focus on ensuring the police have the skills and training to make use of the huge volume of data that is available."

Discussions over the plan have continued. "The reality is that the technology changes fast and that issue has not gone away," Downing Street told the *Financial Times*.

INFORMATION SECURITY

EU Delays Vote on Data Protection Again

The civil liberties committee of the European Parliament met in early May to discuss the latest draft of Europe's Data Protection Regulation, expecting to vote at that time. Instead, after German Member of Parliament Jan Philipp Albrecht observed that more discussions were needed before the draft was indeed final, the committee decided to delay the vote until the end of May.

PC Advisor reported that Albrecht, who is responsible for shepherding the legislation through to the final vote, said he believes that compromises can be adopted with a broad consensus and be ready for the vote before the summer recess in July.

The goal is to create one regulation that replaces 27 national data protection and privacy laws. More than 4,000 changes to the draft text had been put forward in Parliament. In the end, though, the commission predicts the revised regulation will save industry €2.3 billion ($3 billion U.S.) annually.

CYBERSECURITY

U.S. and UK Universities: Welcome to Cybersecurity 401

The best way to beat a hacker is to be a hacker. Seniors at the Polytechnic Institute of New York (UNY-Poly) are learning how to be "white-hat" hackers, experts with hands-on experience to help businesses and government agencies protect their data from cyber attacks.

"It's the new espionage," Evan Jensen, a senior at UNY-Poly, told Associated Press's Jake Pearson. "Spies operate from behind keyboards now." Jensen is one of the leaders of the university's "Hack Night" events where a group of students meet weekly to hone their hacking skills.

Of course they aren't really hacking; that would be illegal. But professors and industry experts collaborate to create exercises that emulate real-world hacking scenarios. Dan Guido, a cybersecurity expert and UNY-Poly's very own "hacker in residence," uses China's 2011 attack on Google e-mail accounts – many of the details of which have been made public – as a case study. The students have to map out, step by step, how the hackers accessed a desktop computer and broke into the company's network.

While Georgia Tech, Purdue, and Carnegie Mellon are well known for their cybersecurity programs, some experts consider UNY-Poly to be among the best programs because of the hands-on, mission-critical, cybersecurity skills the students are gaining, writes Pearson. Not surprisingly, these students' job prospects are extremely good. A 2012 report conducted by the SANS Institute, a cybersecurity training organization, stated that the Department of Homeland Security alone needs 600 cybersecurity experts, preferably with real-world training.

Across the pond, two universities will also offer graduate studies in cybersecurity this fall in support of the UK's national cybersecurity program. The government's National Security Strategy classifies the cyber attack on the same tier-one level as terrorism. The programs are being developed by Oxford University and the University of London's Royal Holloway, thanks to a total of £7.5 million (approximately $86 million U.S.) in funding from the UK's Department for Business, Innovation, and Skills and the Engineering and Physical Sciences Research Council.

The BBC reported that the Oxford program will study security issues related to big data as well as "cyber-physical security," "the idea that cyber security and physical security need to be addressed together rather than separately." It will also research computer verification systems. Royal Holloway's program will work with about 30 businesses and organizations in the security field.

According to Keith Martin, director of Royal Holloway's Information Security Group, this "represents a significantly different approach to research training."

INFORMATION SECURITY

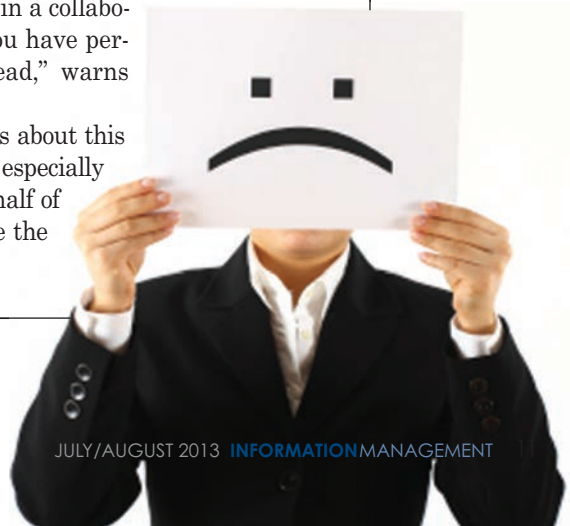
Beware the Enemy Within

A recent study of UK organizations revealed that 83% experienced a data security issue last year. The majority (58%) of those incidents came from within the extended enterprise and may have involved employees, ex-employees, or trusted partners.

The study, "The Enemy Within," was conducted by Clearswift, a cyber-protection software company. The survey focused on the internal threats affecting UK organizations, a contrast to most studies that have zeroed in on external threats. Most internal threats are malicious attempts or stem from poor business processes or human error. Clearswift maintains they are due largely to a lack of awareness of security policy as well as the increasing use of personal devices for work purposes.

"Combine this with the increased uptake of cloud-based tools and reliance on the extended enterprise in a collaborative working environment and you have perfect security storm conditions ahead," warns Clearswift.

Organizations need to get serious about this internal threat, the report concluded, especially because the survey discovered that half of local government bodies do not have the resources to deal with the problem.



ARCHIVES

UK Libraries Build Digital Archive

Six legal deposit libraries in the United Kingdom have begun building an archive of digital content. Regulations were passed in April that allow the libraries to collect and archive such digital content as websites, blogs, electronic journals, and other digital publications. Specifically, the legal deposit regulations give the six libraries the right to receive a copy of every UK electronic publication, "starting with freely accessible websites on the .uk domain, estimated at 4.8 million websites," reported *FutureGov* magazine.

The libraries will employ web-crawling software to store snapshots of 200-500 websites that have been identified as being important for research. These sites will be harvested on a monthly or weekly basis, while others will be captured once a year. Publishers will also be able to submit their material for deposit using a secure deposit portal. According to *FutureGov*, a pilot process has been developed to collect e-books in the ePub format.

The six deposit libraries include the British Library, the National Library of Scotland, the Bodleian Libraries at Oxford University, and the Cambridge University Library. The content will be available to researchers online and onsite via reading rooms at each library. Results of the first year's collection efforts are scheduled to be available to researchers by year end.

"Legal deposit arrangements remain vitally important," said UK Culture Minister Ed Vaizey. "Preserving and maintaining a record of everything published provides a priceless resource for the researchers of today and the future. So it's right that these long-standing arrangements have now been brought up to date for the 21st Century, covering the UK's digital publications for the first time."

FACTOID: Legal deposit regulations for print publications have been in place in the United Kingdom since 1662.

CYBERSECURITY

South Africa Institutes Australian iCode

South Africa recently became the second country to implement network-level protection for end users. The Internet Service Providers' Association (ISPA), South Africa's Internet industry body, developed the voluntary code of practice, iCode, in conjunction with Australia's Internet industry, which pioneered the approach in 2010.

According to ISPA, the code was designed primarily to protect the privacy of end users, not violate it. "The network-level scanning that allows ISPs to detect signs of infected machines does not in any way involve looking at what users are doing online."

The code consists of four main elements: a notification/management system; a standardized information resource; a comprehensive resource for ISPs to access the latest threat information; and a mechanism for reporting back to national security agencies in cases of extreme threat.

"By providing plain-English communication about cyber threats, as the iCode requires, ISPs will help inform the public. They will also help customers who are frequently infected to develop simple and effective safety strategies," the ISPA says.

ISPs that have adopted the code will display a "trust mark" on their websites and other materials.

INFORMATION SECURITY

How Well Prepared Are You for a Data Breach?

According to a recent study by the Ponemon Institute and Experian Data Breach Resolution, 52% of U.S. companies have experienced more than one data breach in the past two years.

If your company is like the overwhelming majority of those that responded to the study, there's a great deal you can do to be better prepared for a data breach. For example, do you require employees' mobile devices (including smartphones and tablets) to be tested for security purposes before connecting to the company's systems? The Ponemon study found that although 78% of companies allowed employees to bring their own devices to work, one-third don't require they be tested; another 28% are not sure if they have such a requirement.

Nearly half (44%) of the respondents said their organization effectively authenticates and otherwise ensures appropriate access to their information systems. Only 43% said their organization promptly changes network access rights when an employee leaves the company. This becomes even more alarming when only one-third of companies are actively monitoring for unusual traffic and other risk indicators.

Following a breach, most organizations could improve how well they communicate the incident to their customers. Just 30% of companies actually train their customer service representatives on how to answer questions about a breach.

"Based on the findings of this research, many organizations are losing opportunities to reduce the risk of negative opinion and loss of customer trust by not focusing on communications with victims," the survey report concluded.

Clearly there is a lot of room for improvement in the majority of U.S. companies. A good place to start, according to *Corporate Counsel*, is by addressing many of the gaps highlighted here.

Cyber-liability insurance may be advisable as well, especially for smaller companies. Symantec reported in April that cyber attacks on businesses with fewer than 250 employees increased 31% in 2012 following an 18% increase in 2011. This is testament to the reality that small businesses typically don't have adequate security infrastructure for protecting financial information, intellectual property, or customer data.

An article in *CFO* magazine reported that small businesses in high-risk industries, such as high technology, financial services, and health care, are "taking out insurance policies to bolster their protection from the potentially crippling costs that can accompany data breaches and other cyber attacks."

Larger organizations tend to have a risk manager and a strong IT department to help reduce the risk and liability. Smaller companies, on the other hand, may only have a chief financial officer or chief operating officer that doubles as a risk manager.

According to Ethan Miller, an attorney at Hogan Lovells, cyber-liability insurance policies usually cover costs incurred by first-party claims, such as the loss of trade secrets and intellectual property. They also cover damages a company pays when involved in a third-party claim. Miller told *CFO* that most policies also include business-interruption coverage in case of a denial-of-service attack whereby the insurance company would provide payment reimbursement for expenses related to such an attack. Such costs, he said, "can sometimes be a life-or-death issue for smaller companies."

Cyber-liability insurance policies are not a solution; they are only a way of minimizing the financial damage. Companies still need to diligently manage their cybersecurity risk, including implementing sound data-protection protocols and employee education. "[T]he insurance company is going to demand you take these protections as part of the application, so as a practical matter you can't become complacent or you'll violate the policy," Miller stressed.

PII

Millennials: Online Privacy Is Dead

A new study by the University of Southern California (USC) suggests the Millennial generation (ages 18 to 34) has a concept of privacy different from that of their parents and grandparents.

Millennials are more willing to allow companies to track them or access their personally identifiable information (PII) if they receive some benefit, such as coupons. Indeed, 51% of Millennials said they would share PII with companies as long as they got something in return; 40% of those older than 35 felt the same way. The younger respondents are also more open to targeted advertising and, not surprisingly, are more active on social media than their elders.

"It's not that they don't care about [online privacy] – rather they perceive social media as an exchange or an economy of ideas, where sharing involves participating in smart ways," said Elaine Coleman, managing director of media and emerging technologies for Bovitz, the research firm that conducted the survey with USC.

INFORMATION TECHNOLOGY

Britain's MI5 Scratches New Digital RM System

MI5, Britain's top intelligence agency, abandoned its multi-million dollar IT project that would have integrated intelligence data and analysis across all the government departments that feed into the agency. The project goal was to make the agency better equipped to deal with new global security threats.

The new system would have pulled together intelligence gathering and searches of paper archives using the latest digital technology by the beginning of the 2012 Olympics in London. Despite the adding of IT experts and the hiring of a team of expensive consultants, the project floundered, leaving the agency with its outdated system. *The Inquirer* reported that earlier this year the project was re-evaluated and the decision made "to admit failure and restart with a new generation of IT specialists," a decision that is estimated to result in losses of £90 million (more than $1 billion U.S.).

Before leaving his position, Sir Jonathan Evans, MI5's former director general, reportedly told the Commons Intelligence and Security Committee that the project's delay was acceptable as the system was not urgently needed.

CYBERSECURITY

U.S. Navy Is Serious About Cybersecurity

Despite budget cuts and the sequester and other funding obstacles, the U.S. Defense Department's cyber program has continued unabated, according to Admiral Jonathan Greenert, the chief of naval operations, who spoke to Reuters.

"The level of investment that we put into cyber in the department is as protected or as focused as it would be in strategic nuclear," Greenert said. "It's right up there in the one-two area above all other programs."

The effort makes sense, considering how heavily the U.S. Navy depends on computer networks and satellites to coordinate personnel, ships, and planes.

"Many people who look at the future of warfare say it's bound to start in cyber. The first thing you'd want to do is shut down their sensors, interrupt their power grid, confuse them…and presumably guard against that kind of thing and recognize it if it's starting," he added.

Greenert's comments came shortly after the Pentagon filed its report with Congress that accuses China of trying to break into U.S. defense computer networks. In addition to China, Greenert said Iran has a "deliberate and emerging" cyber capability, Russia is "very advanced," and North Korea is in the "development stage."

As part of its contingency planning in case of a serious cyber or physical attack on military and intelligence satellites, the Navy is looking at using high-frequency relays employed during the Cold War. The energy blasted from ships by radar and satellite is like a beacon, the admiral explained. Reducing the electronic signature is a key part of the Navy's cyber strategy.

Using radar in targeted patterns, changing frequencies, and shorter pulses are also part of the plan, along with shutting down the systems quickly when in "mission control mode."

"It's like quitting smoking," Greenert said. "You've got to learn to get off this addiction to constant information to and from. Going off the grid can be a good thing."

PII

Australian Privacy Commissioner: Get Ready Now

Australian businesses and government agencies need to get serious about privacy, warned the nation's privacy commissioner and attorney general.

A recent survey conducted by McAfee revealed that 59% of the employees responsible for managing customers' personally identifiable information (PII) were unaware or unsure of the changes contained in the Australian Privacy Act. The new regulations, which become effective next March, levy large fines – $340,000 for individuals and $1.7 million for corporations – if consumer PII is not adequately protected.

The privacy commissioner and attorney general have warned businesses that they need to prepare now for the impending changes, reported *ZDNet*.

Honorary Associate Professor Terry Beed, from the University of Sydney Business School, asserts that a lot of consumer information is being gathered by researchers in a way that doesn't meet the code that governs data collection. Market research tools are readily available to individuals or firms who have no background in market and social research and therefore may not use the data correctly or ethically.

"The ground is changing under our feet," said Beed. "There has been an explosion in the amount of personal data being gathered in the digital environment, and it has revolutionized the way we go about marketing goods and services."

Data Management New Top IT Concern for Accounting Pros

According to a recent study, managing and retaining data rose to the top of the list of IT concerns for accounting professionals in the United States and Canada. Second on the list for both countries is securing the IT environment, which had been the primary concern cited for the previous nine years.

These were the key findings of the 2013 North America Top Technology Initiatives Survey conducted by the American Institute of Certified Public Accountants (AICPA) and the Charter Professional Accountants of Canada (CPA Canada). Nearly 2,000 accounting professionals participated in the survey, which was designed to "dive further into the core concerns and priorities" that AICPA members have regarding IT. This was the first year the survey was conducted jointly in the United States and Canada.

"While survey respondents see data as a key differentiator for businesses, they are less confident in their organizations' ability to successfully address several underlying technology priorities than they were a year ago," according to AICPA's press release announcing the results of the study. Last year, the majority of U.S. respondents reported they were successfully meeting goals in eight of 10 top initiatives; this year, it was only two initiatives – data management and security.

"The good news is that accounting professionals in both the United States and Canada feel comfortable in handling what they view as their two top priorities for [2013] – data management and IT security," said Jeannette Koger, director of member specialization and credentialing for the AICPA.

Ranking of Top Technology Initiatives, U.S. and Canada

(Percentage shown is respondents' confidence level for successfully addressing this priority)

United States	Canada
1. Managing and Retaining Data (**55%**)	1. Managing and Retaining Data (**57%**)
2. Securing the IT Environment (**51%**)	2. Securing the IT Environment (**56%**)
3. Managing IT Risks and Compliance (**47%**)	3. Enabling Decision Support and Analytics (**33%**)
4. Ensuring Privacy (**45%**)	4. Managing IT Risks and Compliance (**57%**)
5. Managing System Implementation (**44%**)	5.Governing and Managing IT Investment and Spending (**38%**)
6. Preventing and Responding to Computer Fraud (**44%**)	6. Ensuring Privacy (**53%**)
7. Enabling Decision Support and Analytics (**37%**)	7. Managing System Implementation (**47%**)
8. Governing and Managing IT Investment and Spending (**38%**)	8. Leveraging Emerging Technologies (**22%**)
9. Leveraging Emerging Technologies (**27%**)	9. Preventing and Responding to Computer Fraud (**47%**)
10. Managing Vendors and Service Providers (**47%**)	10. Managing Vendors and Service Providers (**42%**)

Source: AICPA and CPA Canada's "2013 Top Technology Initiatives Survey"

PRIVACY

Apple's Privacy Headache Intensifies

Apple is taking heat for its privacy policy in both Germany and the United States. On April 30, a Berlin court ruled that Apple's privacy policy violates Germany's privacy law. Apple must either change its policy or appeal the decision.

In 2011, the Federation of German Consumer Organisations (VZVB) accused Apple of "unfair contractual clauses" in its privacy policy, according to *PCWorld.com*. The company eventually changed five of the 15 clauses that were cited by VZVB, but the federation was not satisfied. In 2012, VZVB filed a lawsuit against the software giant. In response, Apple committed to changing two additional clauses, but the VZVB contended the policy still violated German law. The court agreed.

Apple's German privacy policy, which is similar to the U.S. policy, gives the company broad and unspecified use of customers' private information. It also allows Apple to use the personal information for the issuance of gift cards. German law, however, requires that a company advise customers of exactly what personal information would be used and for what purposes.

As of press time, Apple had not commented on whether it would appeal the decision or change its policy accordingly.

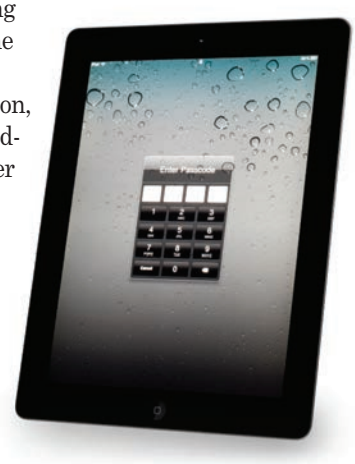
Meanwhile, in the United States, privacy watchdog group Electronic Frontier Foundation (EFF) blasted the technology giant for its lack of transparency with its privacy policies. According to the EFF, Apple could be freely giving up user information to the government. Apple was one of four companies the EFF cited for its lack of transparency; the others were AT&T, Verizon, and MySpace.

EFF cited the four after evaluating 18 companies on six criteria:

- Whether a warrant was required for content of communications
- Whether the firm tells users about government data requests
- The availability of published transparency reports
- Published law enforcement guidelines
- A public record of fighting for user privacy rights in the courts
- Whether the firm supports efforts in Congress to protect privacy rights

The news for Apple wasn't all bad, though. EFF recognized it and AT&T for being members of the Digital Due Process coalition, a group that advocates for user privacy issues in Congress. Only Twitter and *Sonic.net* received gold stars for all six criteria.

END



Who has your back?

	Requires a warrant for content	Tells users about gov't data requests	Publishes transparency reports	Publishes law enforcement guidelines	Fights for users' privacy rights in courts	Fights for users' privacy rights in Congress
Amazon	★	★	★	★	★	★
Apple	★	★	★	★	★	★
AT&T	★	★	★	★	★	★
Comcast	★	★	★	★	★	★
Dropbox	★	★	★	★	★	★
Facebook	★	★	★	★	★	★
FourSquare	★	★	★	★	★	★
Google	★	★	★	★	★	★
LinkedIn	★	★	★	★	★	★
Microsoft	★	★	★	★	★	★
MySpace	★	★	★	★	★	★
Sonic.net	★	★	★	★	★	★
SpiderOak	★	★	★	★	★	★
Twitter	★	★	★	★	★	★
Tumblr	★	★	★	★	★	★
Verizon	★	★	★	★	★	★
WordPress	★	★	★	★	★	★
Yahoo!	★	★	★	★	★	★

Source: Electronic Frontier Foundation "Who Has Your Back?" reports: 2011, 2012