



DATA PRIVACY:

MONTHLY HIGHLIGHTS

| DON HARRIS

The Domestic Front.

October saw a plethora of regulatory and judicial activity in U.S., including developments relating to the No-Match Rule, E-Verify, the Red Flag Rules and GINA, as well as significant actions by the EEOC, a Ninth Circuit warning on return-to-duty physicals and a jury award of \$1.8 million for privacy invasion experienced by one employee. One survey revealed significant costs involved in complying with the new Massachusetts data security regulations, while another showed that privacy and security officers were faring pretty well, the recession notwithstanding.

The International Scene.

FTC took its second public Safe Harbor enforcement action in as many months, taking on six companies that let their certifications lapse (corporate officers, take note). The European Commission announced key issues in its 2010 review of the Directive and also stepped up pressure on the UK government over online behavioral targeting by Phorm. Europe's top privacy regulator called his fellow Dutch "naïve" about privacy, highlighting significant differences in privacy perceptions across at least some EU member states.

Survey: Americans Don't Trust Cloud to Store Personal Data.

Asked what they felt about personal data being stored on third-parties' remote computers, 64% of Americans say they don't want their data kept by a third party, according to the latest installment of a biannual security survey by Unisys. The findings parallel the 65% of respondents who say they are "very or extremely concerned" about misuse of personal information.

Multiple High-Profile Snafus Hit Cloud App Users.

Users of popular cloud computing apps were hit with a variety of high-profile problems during recent weeks and months, prompting Network World to call 2009 the “[Year of the Cloud Outage](#)”. Sidekick users lost access to their data; Gmail suffered its second outage of the month; Twitter was knocked down for many hours by a denial-of-service attack; eBay’s PayPal system crashed; and the list goes on. Also during October, Microsoft warned hundreds of millions of users of [Hot-Mail and Windows Live](#) to change their passwords following a breach. [Gmail and other web-based email providers](#) were also targeted during the month, with thousands of accounts successfully compromised.

54% of Companies Ban Facebook at Work

According to a [study commissioned by Robert Half Technologies](#), 54% of companies ban employees from using Facebook, Twitter, LinkedIn and MySpace while on the job. 19% allow use of social networking sites for business purposes only, 16% allow limited personal use and only 10% allow full access. Another survey in July showed that employee productivity drops 1.5% at companies that allow full access to Facebook during work hours. Results for [Canadian companies](#) showed greater restrictions on access to social networking sites, and separately the Ontario Privacy Commissioner cautioned that [banning use of such sites could backfire](#) by being subverted. 🌐

About the Author: Don Harris is a Global Data Privacy Expert with Jeitosa and the President of HR Privacy Solutions. He has over 20 years of experience and is internationally known expert, author and speaker on HR data privacy issues. He can be reached at don.harris@jeitosa.com.