

Mind the GAPP: Accountants bring GAAP-like principles to the privacy sphere

Jay Cline

December 6, 2007 ([Computerworld](#))

If you haven't heard of the Generally Accepted Privacy Principles (GAPP), take stock: They're likely to become the most important new source of requirements for your IT projects since Y2k and Sarbanes-Oxley. Why is this? The accounting industry has closed ranks around the idea that the GAPP is the best international framework for assessing the privacy health of an organization. So when it comes to IT projects, any system or related business process touching personal data will have new rules to play by.

What is the GAPP? I have to agree with the auditors on this one. It's the best attempt so far to address the main point of pain for global chief privacy officers: the growing complexity of privacy regulations around the world.

The GAPP is a framework that bridges the differences between North American, European and Asian privacy standards through a set of privacy principles common to all. If a company addresses the relevant criteria under each principle, it can simplify its approach to meeting the key requirements of most of these national privacy laws. ([See table for the GAPP principles.](#)) Simpler means lower legal fees and less system rework.

So is the GAPP a plot of the EU, the people who brought us privacy as we know it? Surprisingly not. It's the creation of the American Institute of CPAs ([AICPA](#)) and the Canadian institute of CAs ([CICA](#)). It's not very often that history allows a small group of people to define a profession for generations to come, but that's what may have happened in 2002 when these associations formed a joint privacy task force. Comprised of external and internal auditors, sole practitioners and academics, their goal was to hammer out a common set of rules for building and auditing privacy programs.

By 2006, the resulting framework had won the support of [ISACA](#) and the Institute of Internal Auditors ([IIA](#)). Including the AICPA and CICA, these groups represent over 650,000 professionals worldwide. This is what I mean by closing ranks. Love it or hate it, the GAPP is going to be the standard by which your company's privacy is measured.

"I expect to see more and more companies adopting the GAPP in the future," Sagi Leizerov told me. Leizerov is with Ernst & Young's privacy practice and a member of the AICPA privacy task force.

"One key reason for that is the increased interest and prevalence of privacy audits," he continued. "Considering that the GAPP is the central criteria used by auditors, it will impact CPOs, who will increasingly turn to it when they build their privacy programs."

Who've been the first-movers to adopt GAPP, so far? Leizerov sees large, U.S.-based multinationals filling that role. Steve Kenny, who is with KPMG's privacy practice in the U.K., agrees. "GAPP is being used by a growing number of U.S. organizations," he said.

"GAPP is gaining momentum because it's a pragmatic framework to baseline a privacy compliance program," Kenny added.

Microsoft is one of the framework's pioneers. "We used GAPP to develop our internal privacy policy," said Kim Hargraves, director of strategy and risk management within the company's Trustworthy Computing division. "It's fairly comprehensive in its scope, yet allows for the development of programs around it that can protect sensitive data, put customers in control of their personal information and support compliance with various legal requirements across the globe."

Everett Johnson, a former Deloitte & Touche partner and chair of the joint task force, thinks Microsoft got it right. "In addition to being a tool for auditors," he told me, "GAPP also is very helpful for designing a comprehensive privacy program or for benchmarking an existing privacy program."

McLean, Va.-based Freddie Mac is also an early adopter. According to Britt Murray, the lender's CPO, "Organizing our internal privacy policies and standards around GAPP has enabled us to adapt to new laws without needing to restructure our existing standards or create new one-off standards."

"From a regulatory compliance view," Murray added, "it's easier to make changes when they fit nicely within an overall framework that is already familiar to the business areas."

But what will it take for the GAPP to attain the pre-eminence of its financial counterpart, the Generally Accepted Accounting Principles (GAAP)? Critics say that multinational CPOs were not sufficiently involved in the process of creating the framework, and without their input, it's premature to append the "Generally Accepted" label to the GAPP.

More refinement of the framework may also be in order. "European organizations are more resistant to adopting GAPP," Kenny explained, "largely because GAPP was not intended to formally provide assurance against EU member state data-protection legislation."

Notwithstanding these two hurdles, I think the GAPP will take off when something else happens: when multinationals start requiring their partners and suppliers to meet GAPP standards in order to process or host personal information. Vendor-assurance programs for PCI-covered entities were the channel in 2007 for making the PCI Data Security Standard the lingua franca of information security. The degree to which the GAPP is incorporated into these programs will also be the harbinger of how quickly the framework is propagated around the world.

Multinationals would do well to throw their weight behind the GAPP. If they take a wait-and-see approach, they risk opening the door for a more onerous standard to emerge, such as through the International Standards Organization. And lawmakers, with no internationally recognized reference point on privacy, will continue to make CPOs' lives difficult.

Jay Cline is a former chief privacy officer of a Fortune 500 company and now president of [**Minnesota Privacy Consultants**](#). You can reach him at [**cwprivacy@computerworld.com**](mailto:cwprivacy@computerworld.com).