

Privacy software: Who are the early leaders?

Jay Cline

August 12, 2010 ([Computerworld](#))

Anybody responsible for data privacy soon discovers a hard truth -- privacy compliance is a highly manual undertaking. Whether it's tracking where all of the company's data is or keeping up with changes in obscure privacy laws, the privacy professional is often sentenced to a life behind spreadsheets. If privacy didn't deal with cutting-edge social issues, it might contend for the most tedious job in the corporate center.

But the tedium may be lifting.

The privacy profession, which just 10 years ago fit into a single conference room in Washington, has grown large enough to form a reliable market for software products. When in 2006 I first estimated the North America-dominated privacy-advice market at \$400 million, membership in the International Association of Privacy Professionals (IAPP) stood at 2,000. The IAPP now has over 6,000 members, according to its [recent paper](#) on the future of the privacy profession. Other benchmarks such as the number of privacy consultants and lawyers suggest the world privacy-advice market is now around \$1 billion.

A handful of software entrepreneurs has noticed. Together they form what I'd call the "privacy GRC" market, where *GRC* stands for "governance, risk and compliance." GRC makes up most of what privacy people do.

It's not a big market. To put things into perspective, Gartner is only in its third year of [analyzing](#) the nascent IT GRC market. The privacy GRC market is at the moment no more than just a subset of that.

Nonetheless, the number of privacy GRC products is growing. Over the past year I noticed more of these booths at the privacy conferences I

attended. So I commissioned research analyst Michael Lotti to help me investigate.

What did we find?

1. Foundational regulatory mapping and policy features

One of the biggest pain points of the privacy officer is the continued churn of new privacy regulations. Global corporations are now subject to an overlapping web of data privacy and security laws and standards. To cope, their privacy staff are busy tracking legislation and mapping the common requirements in each law to a set of unified control statements. An example of a control statement is "encrypt sensitive data transmitted outside Company networks." The privacy people -- months later, usually -- then group these controls into [enterprise](#) policies.

Most of the tools that Michael and I looked at -- including those from Archer, brinQa, Agiliance, ControlCase, Avior Computing and Consult2Comply -- automate this chore, albeit to varying degrees. Among these, Consult2Comply stands out from the crowd for the number of regulations mapped and the flexibility of how to reorient the mapping to your own needs.

The main question that privacy staff considering these applications should ask is: Which tool does regulatory and policy mapping at the right level of detail for my organization? A risk-averse or regulated company, for example, would tend to want the highest level of granularity that enabled it to demonstrate regulatory compliance. A sales-oriented culture, meanwhile, might want only high-level mapping that facilitated more of a risk-based approach to policy making. With that in mind, none of the tools, with the possible exception of Consult2Comply, seems to offer a way to easily dial up or down the granularity of its mapping. And none really comes out of the box with canned sets of control frameworks for privacy-intensive parts of organizations such as direct marketing and call centers.

2. Reliable privacy-assessment functionality

Another pain point for privacy offices is overlapping assessments. Service providers in particular now endure a never-ending gauntlet of client privacy and security audits. Many supplement these with their own internal audits and information-risk assessments. As a result, a privacy office and internal audit department may end up asking and answering the same questions dozens of times a year, yet lack an integrated view of all of the assessment and audit results. Imagine taking the same final exam from 20 different professors, receiving different grades, and never graduating from the class.

The privacy GRC applications we reviewed would address the core part of this conundrum. All of the tools that included a regulatory mapping feature also incorporated a usable framework for conducting integrated risk and compliance assessments. The leaders in this area -- brinQa, Agilience, Avior, ControlCase, Archer -- enable you to assign a weight to each assessment question, attach supporting documents to each answer, and parse out and e-mail questions to different people across a department. They map the questions back to the underlying regulations, enabling you to answer a question once instead of a dozen times. Of these, brinQa stood out for its vision to pull information from other enterprise tools -- such as centralized-log consoles and data-loss-prevention scans -- into one integrated spot. These tools have obviously learned from the audit features of ThomsonReuters' [Paisley AutoAudit](#), a leader in internal-audit software.

But auditors and compliance managers may need more out of these platforms. Brian Tretick, former co-leader of Ernst & Young's privacy practice and now head of [Athena Privacy](#), told me there is a gap in the market for quantifying privacy risk. "One of the big challenges in using privacy-assessment templates is converting assessment gaps into a risk measurement," he said.

"People don't know how to factor in the concept of likelihood of privacy-regulatory enforcement into risk ratings," he elaborated, "and some organizations mistakenly say that if there is a regulation on an issue, and

it's not met, it must be high-risk. Privacy risk and compliance is not there yet."

3. Sufficient data inventorying features

Maintaining a complete and current data inventory is another elusive goal for most organizations. Why? Data seems to be everywhere and always changing. Even the best privacy people -- those triathletes who combine the skills of the privacy attorney, system administrator and records manager -- often suffer the fate of Sisyphus. He was the king of Greek mythology consigned to rolling a rock up a hill only to watch it roll back down, over and over through eternity.

Three of the products we looked at -- Archer, brinQa and Agiliance -- would lower the slope of the hill of Sisyphus. They provide ways for multiple users to continually update a common source of truth about the organization's stores of data. The Jordan Lawrence offering in particular stands far above even these in the number of record types, storage types and other data elements it tracks, in addition to providing multi-user updating. It really doesn't have a peer.

All of this said, none of the products has yet found the magic of converting a data inventory into a data map that graphically shows the movement of data through an organization. Tretick added that privacy officers won't be satisfied with this data-repository approach until it incorporates business-process information such as allowable data uses, privacy consents and data transfers.

4. Cautiously optimistic customers

The privacy GRC market is young, so there is a relatively small client population. We spoke with a handful of customers who we found on our own. We heard two themes: relief at having software to leverage existing staff, but also a sense of being overwhelmed by the Year One task of getting everything loaded into the tool and customized. "More needs to be

pre-populated and pre-cross-referenced," Tretick opined. We also heard grumbling about licensing costs well into the six figures.

I asked Michael which were his top picks for overall usability, and he said Archer, brinQa and Avior. My opinion? All of them have a long way to go before they could be the CPO's dream product. But each is a significant improvement over the days of doing privacy by spreadsheet.

Early privacy GRC contenders

The privacy governance, risk and compliance niche is a subset of the IT GRC market and is characterized by privacy regulatory mapping, privacy assessments and data inventorying features. The products in the table below are the pioneers.

| Firm | Location | Founded | Employees | Product differentiator | Contact |
|---|------------------|----------------|------------------|---|---|
| <u>Jordan Lawrence</u> | St. Louis, Mo. | 1988 | 40 - 45 | Data inventorying | <u>Marty Provin</u> |
| <u>Archer Technologies</u> (an EMC company) | Kansas City, Mo. | 2000 | 135 | Breadth of feature set | <u>Steve Suther</u> |
| <u>ControlCase</u> | McLean, Va . | 2004 | 55 | Data classification integrated with scanning tools | <u>Hugh Kominars</u> |
| <u>Avior Computing</u> | Nashua, N.H. | 2004 | 24 | User interface | <u>Steve McAlmont</u> |
| <u>Agilance</u> | San Jose, Calif. | 2005 | 50 | Reports and workflow | <u>Arti Arora Raman</u> |
| <u>brinQa</u> | Austin, Texas | 2007 | 22 | Vision for pulling data from other enterprise systems | <u>Hilda Perez</u> |

| Firm | Location | Founded | Employees | Product differentiator | Contact |
|---------------------------------------|-----------------|----------------|------------------|-----------------------------------|--|
| <u>Consult2Comply</u> | Reston, Va. | 2007 | 6 - 15 | Regulatory mapping | <u>Steve Crutchley</u> |

Source: Jay Cline