

Corporate Privacy: An Interview with Michele Drgon

As information security professionals, we are now required to think broader than the technology and must understand the more comprehensive risks that face the companies we work for. In today's global environment it is essential for security officers to effectively partner with business stakeholders to truly be able to build a holistic risk management program. In doing so, one of the most important stakeholders to build a relationship with is the Chief Privacy Officer. The foundations of building any comprehensive risk program must include an understanding of the privacy legislature and its implications.

In this two part series, I am exploring the Corporate privacy landscape with Michele Drgon, the founder and President of DataProbity (www.dataprobity.com), a consulting company specializing in the development of strategic privacy governance programs for major corporations. Michele has been involved in the privacy technology and compliance space since 1998 and was formerly the Senior Director of Data Protection/Privacy at Motorola.

[How has the privacy landscape changed in the past, say, ten years?](#)

There have been so many significant events that have led to the environment today in which privacy is a much-discussed topic in the news and elsewhere. While Europe, Canada and some countries in Asia had enacted broad legislation to protect individuals' personal information, the United States rolled out laws in waves, with each new law protecting a specific type of personal data. First COPPA (Children's' Online Privacy Protection Act), then Gramm-Leach Bliley (Financial Services Modernization Act) and finally HIPAA (Health Insurance Portability & Accountability Act) rules were implemented. Years ago, the perception of individuals was that since "so much information was already out there", they couldn't do anything to protect it. Then, as banks and medical providers started providing privacy promises, individuals were introduced to the concept of privacy rights. When spam laws and "do not call" lists were launched, individuals realized that they were in a position to protect themselves from unwanted communications (going back to Justice Brandeis' original definition of privacy as "the right to be left alone"). Instead of assuming that privacy was synonymous with security, as so often is the case, individuals truly are sensing the role they play in ensuring the protection of their own personal data. They are recognizing the trade-offs between providing their valuable personal data and the potential impact to their lives if that data is misused. Their demand for notification and retribution results from their newly-formed expectation that corporations have a responsibility and an accountability regarding the handling of consumer and employee data.

[How has the rash of security breach laws affected the privacy space?](#)

The good news is that they really underscore the intensifying levels of consumer expectation, putting the onus on the corporations to preemptively notify consumers so that they can put counter-measures in place to protect their identity. The bad news is that the tendency is to assume, once again, that secure IT systems are the “answer” to privacy compliance. Rather, what the breach laws should be catalyzing is a change in corporate thinking regarding the storing of such critical consumer data. This is what strategic privacy governance is all about: designing privacy into the front-end of the data collection process. Why is this data needed? Why must it be stored? What is the real value to the corporation, and the consumer, for having that data resident in a corporation’s database? Marketing leaders should define data collection schemas outlining the appropriate data to be collected for each type of marketing activity or sales transaction. Similarly, Human Resource and Finance management should be doing the same for employee data (albeit, far more sensitive).

Privacy compliance strategy needs to be an end-to-end process, from the point of collection of the data to the point of deletion. The security breach laws put a necessary focus on corporations’ underlying privacy compliance strategy: what was the incremental business value gained by keeping the data – and was that value ever weighed against the risk that that retention posed to consumers, corporate image or bottom line? It’s like putting a tiger in a cage next to a kindergarten. When someone finally breaks the lock on that secure cage and “notification letters” are sent to the parents who run scrambling to protect their children, the biggest question on their minds will be “Why on earth was someone keeping a tiger in a cage in the first place?” And even if their children (or identity) is deemed safe, the panic that they endured will remain on their minds for a long time. So while breach laws require a specific response in the event of a “broken lock”, world-class privacy governance mandates tougher scrutiny of the tigers BEFORE they are “collected and caged”.

[So you’ve mentioned marketing, human resources and finance. Do other departments play a role in privacy compliance?](#)

Yes. An interesting scenario has resulted in the post-Enron era. Sarbanes-Oxley outlined an “adequate internal control structure” requirement in Section 404. Corporate information systems were suddenly thrust into the limelight across organizations with focus on the protection of valuable information assets. Corporations were required to disclose potential risk areas and, particularly as major privacy breaches were in the news constantly, the effectiveness of internal controls for the protection of customer data became a point of interest for an array of C-level executives: Chief Compliance Officer, Chief Governance Officer, Chief Audit Officer etc. It is not unusual to now see privacy compliance as an agenda item at conferences for these types of leaders. In fact, in a recent survey of Corporate Compliance Officers, privacy and information safeguarding were ranked among their Top 10 concerns. Also, many of corporations are blending these roles. One major corporation even has a Chief Ethics, Privacy & Compliance Officer.

[How has technology impacted privacy compliance?](#)

Technology advances present a balance issue for companies. Corporations have the ability to analyze and track their customers' and employees' activities and patterns through the use of ever-evolving technologies. However, where do you draw the line? Once again, this highlights the critical need for a corporation to strategically plan their privacy governance program. Decisions need to be made about the business value of certain data vs. the privacy impact to the individual. We've all heard stories of the rental car companies who charge their customers fines when they discover that a car was driven too fast or out-of-state etc. Weighted decisions need to be made about the intrusive capabilities of these enabling technologies and the privacy rights of the individual. While these decisions might be easier to make relative to customers' data, what about employee data? Technologies exist to alert companies to employee mail that contains certain threat-related words, for instance. Should that employee be monitored? What about the use of GPS and other tracking technologies? Definitions should be created, in collaboration with the Ethics and Legal departments, outlining the level of "appropriate granularity" of scrutiny relative to each level of perceived threat. These privacy strategies should then be reflected in corporate policies.