



Jay Cline

President
Minnesota Privacy Consultants



Brian Tretick

Managing Director
Athena Privacy

Privacy and Data Protection Compliance Metrics: Is it time?

In today's business world privacy and data protection compliance is a state of becoming, rather than being. Accountability and governance are terms that imply responsibility and oversight on the part of a company that is constantly changing within an economy, global or local, that is also in a constant state of flux. With the ability to measure compliance to regulations; to policy; to performance to customers a company can know where it is in its quest to become compliant in a manner that they and their jurisdictions define.

Such a vision of measured compliance is no different than the production of an annual report to the board of directors and shareholders about the financial fitness of the corporation. It is no different than the controls applied as required by the Sarbanes-Oxley Act. The measured compliance is, however, about the privacy and data protection fitness of the corporation.

Jay Cline, President of Minnesota Privacy Consultants, and Brian Tretick, Managing Director for Athena Privacy, provide us with some insightful and thought-provoking answers to key questions about measured compliance. Before his ten-year career in privacy, Jay worked as an economist, and so sees privacy through the lens of numbers and graphs. Brian has been a management consultant since birth, and looks to process effectiveness. It takes a firm grasp of the numbers and a detailed understanding of the process, in light of the data and the business, to measure.

Nymity: Some people say you can't measure privacy, so why bother. Do you agree?

Cline: I think you can measure everything except love. Anything that a business does should be measurable, or it's not worth doing. Businesses survive by creating value. If a privacy program isn't creating measurable value for the business, it should be shut down and converted into a nonprofit venture. When Peter Cullen, now Microsoft's chief privacy officer, was at Royal Bank of Canada, he quantified privacy's contribution to the RBC brand at 7%. That's what we need to do.

Tretick: I agree with Jay completely. I think the big challenge is that the people doing privacy just don't have the training and experience in measuring privacy as well as they need. But we cannot leave it that way any longer. It is time that privacy got done better, more effectively, and with accountability. You need measurements to demonstrate all that.

Nymity: Why are privacy and data protection metrics so hard? Why are privacy and data protection metrics so intriguing?

Tretick: The thing with privacy is it gets involved everywhere you process personal information, and that can be in nearly every business process. So, in effect, measuring privacy involves measurements across the enterprise. Sometimes that's just too vast to get our brains around.

Cline: These kinds of metrics are hard I think for two reasons. First, we can't agree on what we mean by 'privacy' -- even in your question you had to add 'data protection' -- so we lack a shared starting point. Second, there isn't often a direct cause and effect between privacy and the cash register. It takes more time to find how privacy creates value than it does for, say, the sales function. If I'm in sales, I can say that my phone calls this quarter generated \$1 million in new business. It's harder for me to show that doing privacy right on our websites generated a 10% lift in purchases or loyalty-program enrollments, or doing privacy right in our direct marketing generated consumer profiles that were 25% more valuable and enabled 10% more up-selling and cross-selling by call-

center reps. It's because doing privacy right often tends to go along with doing something else well at the same time that will take credit for the ROI.

Nymity: What is 'measured privacy and data protection compliance'? Is it about compliance to regulations; to policy; to performance to customers? What metrics does it include? Is there such a thing as privacy ROI?

Cline: All of these questions hinge on there being a personal-data ROI. Your typical business-to-consumer company in the Fortune 500, for example, is sitting on top of mountains of consumer records that have a half life similar to uranium. To the extent a privacy program can generate consumer trust that leads to more deposits of data, extends the half life of data, protects data from loss or error, or unlocks new data uses, a privacy ROI most definitely can be calculated. That ROI will differ for business-to-business companies where the ROI is based on sales, government agencies where the ROI is use of services, and academic institutions where the ROIs are student satisfaction and alumni giving. The more complete approach for all of these business models would be to talk of an ROI to *data management* – or 'information governance', if you're sitting in a sophisticated Georgetown restaurant with Brian.

Tretick: There are a few obvious and somewhat old school measurements that get us started but are not enough in themselves. The first is—the mandate from the attorneys—is the compliance assessment, which can answer, "at this point in time, are we compliant with some set of rules?" Mark them green for yes, red for no, and yellow in the cases that there are certain improvements to be made. The second is in the jurisdiction of auditors. It can answer whether specific controls are in place and operating effectively, normally again at a point in time. However, as Jay noted, these cannot measure business value or performance enablement because of the thing called privacy.

Nymity: How does a company determine which metrics are important?

Tretick: Jay and I have been discussing this at length. There are a number of different dimensions that make sense. First, in the risk management and compliance dimension, you really should know how you stack up, what effect all your risk management and compliance functions are having. Next, in the control dimension, you should know how well the specific controls over personal information are actually performing. A big challenge is that privacy controls span the business, they aren't under the jurisdiction of just one group, and definitely are much more extensive than just IT controls. From a business perspective, you really should have the hard facts around how your data management or information governance functions affect business performance. Do they enable certain uses of personal information, its transfer to or access by others, or otherwise increase in business value? Finally, you should know how effective the sum of all privacy GRC functions is. Can you show that you are running privacy like a business?

Cline: I think the Balanced Scorecard methodology is the way to go. It's the way to run privacy like a business like Brian was saying. It takes three steps: create a strategy map, assign measurements and target thresholds to each component of the strategy map, and then identify owners of each metric. Doing the strategy map well – which involves identifying the end contribution of privacy to the business, then working backwards from there to identify all the initiatives that the privacy office must undertake to reach that end – is what makes or breaks whether a company finds its meaningful privacy metrics. For example, a strategy map might indicate that if we deploy encrypted e-mail along with an awareness and training campaign, we'll meet our business objective of reducing the cost of data exposures. On the scorecard, there could be three metrics associated with that strategy chain: % of users with encrypted e-mail, % of users completing training, and # outbound e-mails containing sensitive PII.

Nymity: What are privacy pros looking for with metrics? Are there a core set of metrics that companies can begin with to focus on compliance to regulations; to policy; to performance to customers?

Cline: Every worthwhile business activity either reduces cost or increases revenue. Privacy pros I think struggle seeing their program only indirectly generating revenue through boosting brand, or only indirectly reducing cost by mitigating risk. Privacy pros are looking for harder bottom-line metrics such as: we enabled \$10 million in new revenue last year by joining the Safe Harbor, or we retired 20 servers by implementing a data-retention policy, or we reduced cyber-insurance premiums by \$200,000 by improving our compliance scores by 10 points on a 100-point scale. In each of these cases, other business components will be claiming they were responsible for those dollars too. So it'll be up to the CPO to negotiate with these business counterparts ahead of time on what the end message is going to be and how they're going to share credit.

Tretick: A far as a core set of metrics goes, we have today the results of compliance assessments and internal audits. Common measures to report are the number of medium and high priority findings in the assessments, and number remaining open as they age. This is routine for other internal audits as well, so management knows what it is looking at. As Jay said, however, in addition to the open status of risk and compliance, organizations need productivity measures related to privacy: measures about the business value created or sustained through privacy governance functions. Privacy metrics can show business achievements.

Nymity: How do you implement privacy and data protection metrics in a large organization? What are the success factors in implementing privacy and data protection metrics?

Cline: I think identifying the metrics is the easy part. Whether a metrics program is sustained past the metrics offsite depends on getting a sponsor on the executive-leadership team to approve the metrics and agree to receive regular metrics reports. Even with that level of support, the metrics program will only survive past year two if the ELT begins to make decisions based on those metrics.

Tretick: Yes, sustaining them is key, being able to have up-to-date metrics. So, the success factor is in automating the measurements related to what you are reporting. Connecting to source systems, other groups, flirtations with continuous control monitoring and similar approaches, these are what counts. It cannot take days each time to update your metrics. You need formal processes, so the measures are made the same way each time, and you need automation, so as many as can be magically populated are.

Nymity: Where have you seen privacy and data protection metrics really be effective? Did these successful metrics depict a 'measured data privacy and protection compliance' state for a company or were they measuring one component of privacy and data protection? Please provide examples.

Cline: I've seen it work exceedingly well for a software-development company that held a monthly board meeting to make decisions based on their balanced scorecard. They grew the company 300% while their counterparts had flat growth, and they swear by the scorecard. Producing secure software was business critical for them, and this goal was woven into their overall scorecard objectives.

Tretick: Metrics work the best when you are measuring related to a recurring and formal process. One-off measures get floated to management all the time, but they are only point-in-time, issue-based metrics. Metrics that can show performance, value, or completion, that can be tied to recurring processes, are the most useful. Embedded checkpoints and measurements in common processes such as system lifecycle management, employee training and development, new account set up, direct marketing provides the ability not only to see with compliance and risk lenses, but also to see coverage, completion, and trends. So, look for privacy measures that matter in recurring, formal business processes.

Nymity: Is it possible to choose one privacy metric to hang your hat on? If so, what would that be?

Cline: I err on the side of optimism. So I think you can get away with one metric: a privacy-maturity score or privacy-health index, a concept I learned from former Microsoft CPO Richard Purcell. If enough senior executives agree that hitting a certain level of overall privacy maturity is business critical, you have your single metric.

Tretick: I'm okay with that. I like maturity models. They don't say, "We are compliant" or "Our risk is low", but rather they say "We are performing to this level." That shows performance quality, that you are running a mature business function that can take care of compliance and risk issues as they arise. It's better to have a trustworthy process that handles challenges as they come than to know at one point in time you happen to be compliant. So, if there was just one measure, it would be a "How well we are performing our privacy management functions" measure for each major business group and affiliate.

Nymity: Where have you seen privacy and data protection metrics go bad? Why? Please provide examples.

Cline: I've seen a couple variations repeated in different places. A more common one is where a relatively low-level privacy or security analyst develops a fairly solid set of metrics, but doesn't have an executive sponsor who sees the value. So the effort fizzles. Another is where a more savvy privacy director gets the ear of an executive, holds a team offsite to develop the metrics, and populates a first draft. But the care and feeding of the metrics requires other departments to devote staff resources that fade over time, so the metrics report narrows down to a handful of disparate, unrelated metrics such as opt-out rates and the number of breaches.

Tretick: I think it's getting the wrong information to answer the wrong question. Just because you can measure something one way doesn't mean the results will tell you what you should know. Getting the questions right for you is essential. You can measure total numbers of, say, opt-out requests received or employees who have taken privacy training, but what do you get from those numbers. Instead, you might ask, "What is the opt-out rate over time?" or "How has the new messaging in marketing changed the opt-out rates?" or "How well is our privacy training program working." Completion measurements only tell you whether you finished, not how well you did it. Privacy needs to move from not only getting it done, but getting it done well, effectively and efficiently. Our measures should be focused on how well things are getting done.

Cline: I would also say the perfect can quickly become the enemy of the good when it comes to privacy and security metrics. Because privacy can affect so many parts of a business, there can be a tendency to want to take a comprehensive approach and measure, say, 50 metrics. The privacy officer with limited time and resources might be more successful in the long run to start with 10 or 12, and engage in some trial and error in year one before adding new metrics.

Nymity: Are some industries, jurisdictions or corporate cultures further along in the privacy and data protection metrics journey than others? Do any industries, jurisdictions or corporate cultures lend themselves better to privacy and data protection metrics?

Cline: I've seen two types of companies do relatively better than the others when it comes to privacy metrics: those with loyalty programs, and US-based companies trying to expand into Europe. With loyalty programs, it's easier to measure the direct impact of privacy on the amount and quality of customer data and customer interactions. In the second example, it's been my experience that business-development and marketing people in the US hear loud and clear the privacy concerns of their prospective EU clients. As a result, they tend to more highly value the role of the privacy office in helping open new markets for them, and they're more willing to sign off on privacy ROI metrics.

Tretick: Yes, as Jay said, not so much from an industry perspective but rather from the business functions performed. Marketers who have included privacy in their campaign management are probably the most mature. They are using formal, recurring, automated processes. Another area is in technology management: the security of technology assets can often be measured in a recurring and automated manner.

Nymity: What are the differences between privacy and data protection metrics and security metrics? Should they all be part of the 'measured privacy and data protection compliance' metrics program?

Tretick: It comes down to what questions you want answered by the metrics. The big question, "How well are we doing?" can be applied to any part of the business. If you can think of information assets having value, compliance obligations, and associated business risk, you can ask for all information (not just for personal information), "How well are we doing at getting value from our information assets, meeting our information compliance obligations, and managing information risk?" This is bigger than just privacy and information security.

Cline: I think it all blends together, along with data-retention metrics. So we're better off calling the whole thing data-management metrics. Each category you mentioned has an element of revenue generation and cost reduction to it, depending upon what sector the organization is in.

Nymity: In closing is there anything that you would like to share with our readers that we have not asked, such as were there any good books or guidance on the topic?

Cline: There are a number of good books on security metrics, but none really on privacy metrics. The three I'm looking at on my shelf are: Complete Guide to Security and Privacy Metrics by Debra Herrmann (note: it's 90% security and 10% privacy); Security Metrics by Andrew Jaquith, and Quality of Protection by Gollmann, Massacci, and Yautsuihin. I hear a man named Tretick has an interesting Privacy Maturity Model as well.

Tretick: Hmm. I think that maturity is key. Everybody in privacy has done something, right, they have something in place. The business questions that need to be answered involve how well are we doing.