All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Transparency – a different protection objective

Every once in a long time, the field of information protection goes through a sea-change. This may be one of those times. Over many years, a relatively static set of protection objectives, starting with Confidentiality, Integrity, Availability (CIA), and adding Use control and Accountability over time. While we got comfortable, the world got uncomfortable. Meanwhile, the areas of diplomatics, archival science, and library science long held strong to a concept that information protection long ignored as a field. This is the concept of transparency.

What is transparency and why it is important?

Transparency is, in effect, the ability to see what someone else is doing. It comes from transparent, defined as “able to be seen through” and “easy to notice or understand”[1] In the field of records management implementing the principal of transparency is described as: “The processes and activities of an organization’s recordkeeping program shall be documented in an understandable manner and be available to all personnel and appropriate interested parties.”[2] In government we have things like Florida's “sunshine” laws, while state governments have implemented laws like California's SB1386 which required that when personally identifiable information is released to unauthorized parties, notice must be given to those effected. In financial institutions, there are requirements to share information associated with protective measures in order to demonstrate trustworthiness to other institutions and governments. The concept of safe harbor is associated with notice of meeting standards and independent audits of compliance with such standards is often used as a basis for trust. All public companies in most of the world have requirements for transparency with regard to their risk profiles and things that may substantially effect shareholder value, largely as a result of the Sarbanes-Oxley Act and global changes reflective of the results of that act. Accounting has published principals, the GAAP standard, that identifies what is generally accepted in accounting practices and required in accounting for public purposes. These are all elements of transparency associated with the processes undertaken, and they form a basis of trust.

In order to demonstrate worthiness of trust in protection to others, some level of transparency is necessary with regard to processes. Hence transparency is often one of the protection objectives of an organization that wants to do business and exchange information with others. Of course transparency doesn't apply to everything all the time any more than confidentiality does. Public records, for example, are public, and thus confidentiality from the public is not typically the objective. But to assure the public's trust in those records, transparency is necessary. Transparency provides the means by which the public maintains confidence in its government, at least in free societies. The lack of transparency with regard to surveillance programs is an example of how public trust can be destroyed. Transparency is the only way we may have available to determine whether, and to what extent, we can believe what others say, and its loss may lead to a breakdown in the fabric of modern society.

[1] Websters dictionary online

[2] ARMA International’s Generally Accepted Recordkeeping Principles (GARP®)

How big a change is it to add transparency to protection objectives?

In making a change to put transparency on the same level of consideration as integrity, confidentiality, availability, use control, and accountability, we have made a major change that ripples through a wide range of issues. The technologies of transparency are largely related to audit and version control methods, while the tradeoffs between secrecy and transparency become noticed, the need for integrity to assure transparency becomes more interesting as the methods in use become exposed thus driving toward potential release of information that could effect availability.

Duties to protect must now explicitly review these requirements, but that should have been happening anyway. On the other hand, when we consider consequences of protection failures, loss of transparency becomes another factor that has to be considered, and potentially rethought throughout the protection program.

When a company published a policy, transparency is sometimes already included as part of the privacy policy or in other ways, but transparency itself is often not called out. Contracts that embed releases and details in small font and in the middle of a long contract of complex language can reasonably be said to lack transparency. The notion that you make your money by advertising to those who use your “free” services, while often true and seemingly obvious, becomes something to be declared in a public way.

Policy automation includes many methods for taking information on policies from other organizations and automating decisions about sharing and access, and this is integrated into portions of identity management, so policy frameworks become one of the main paths for sharing transparency information. As this is done, decisions about transparency have to get codified into such mechanisms and they may effect the ability to share with organizations that are too transparent or not transparent enough. Information sharing organizations need to start putting transparency requirements or codifying transparency mechanisms so that others can make decisions about their proper use.

To be clear, transparency is not always a key requirement, and in many cases, opaqueness is just fine. Which is to say, the methods of making things opaque is also potentially critical to transparency decisions. If we are providing statistical data or partial records, issues like data aggregation and obfuscation become critical criteria and technology mechanisms. In human experimentation, which is commonly done in information technology without the same controls typically used in other fields, informed consent becomes a transparency issue. For a period of time the details must be kept opaque, but then they must be released. Thus we have lifecycle issues associated with transparency.

Summary

These complexities are the very reason that transparency has to become a fundamental protection objective and get baked into the full range of decisions regarding information protection. But that is not an easy job, and it will take time. Technologies are not typically directed toward this objective. While many may be repurposed to that end, new technologies may have to emerge and new analytical methods be developed to integrate this concept across the information protection space. Transparency, it seems, is here to stay, and it is time we attend to it. We hope you will tell us what you think about this notion and the changes we make to accommodate it in our standards of practice and throughout our thinking.