

September 2, 2011

WRITER'S DIRECT LINE
858.847.6728
aserwin@foley.com EMAILCLIENT/MATTER NUMBER
999999-9999**VIA EMAIL: SEC-CERT@NIST.GOV**National Institute of Standards and Technology
Attn: Computer Security Division, Information
Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930Re: **Foley & Lardner LLP's (on behalf of the Lares Institute) public comment on Appendix J:
*Privacy Control Catalog***

To Whom It May Concern:

Foley & Lardner LLP, on behalf of The Lares Institute, supports and recognizes the significant value and implications of the incorporation of "Appendix J: Privacy Control Catalog" into the 2011 update to Special Publication 800-53, Revision 4 ("Appendix J"). Due to the ever-increasing dependency on information systems and various new technologies, maintaining the confidentiality and integrity of an individual's personally identifiable information ("PII") has become a top concern for many organizations. The structured set of privacy controls provided in Appendix J and the guidance it provides to both public and private organizations in adopting and enforcing best practices for privacy and security, directly addresses the concern of many organizations in maintaining the confidentiality and integrity of PII. We believe the privacy controls identified by the National Institute of Standards and Technology ("NIST") has provided the federal government, as well as many private organizations, a viable framework for ensuring that privacy requirements will be satisfied in a comprehensive, cost-effective, and risk-based manner. In reviewing the draft, however, we would like to offer our observations of how the current effort may be improved.

1. Not All Data is Created Equal

The privacy controls identified in Appendix J provides a robust and thorough approach for addressing and managing highly sensitive PII. However, there is little recognition of the fact that not all data is equally valuable or equally sensitive. Therefore, not all information needs to be protected with the same level of rigor. As a result, the robust privacy controls identified in Appendix J may need to be prioritized and applied proportionally to reflect the sensitivity level of the particular PII being protected. Implementing these detailed privacy controls for all types of PII may be costly and resource-intensive for many organizations. In order to reflect sensible resource allocations and concerns, organizations may want to prioritize what PII may be subject to such thorough privacy controls, and which may not, depending on the sensitivity level of the PII.

On page 1 of Appendix J, it states that "The controls focus on information privacy *as a value distinct from*, but highly interrelated with, information security." (emphasis added). We agree with this perspective on privacy as a value. However, the value allocated to privacy shifts and changes based on demographics and the type of information. In the Lares Institute report entitled, "The Demographics of Privacy – A

National Institute of Standards and Technology
Attn: Computer Security Division, Information
September 2, 2011
Page 2

Blueprint for Understanding Consumer Perceptions and Behaviors,” (September 2011), it was discussed how consumer attitudes and behaviors should be incorporated into privacy designs of companies. Certain clear patterns were identified when demographic issues and privacy were examined. When age was considered, there were some strong correlations between age and general privacy sensitivity, with those in the youngest age category having the lowest sensitivity to privacy concerns. In addition for particularly sensitive data, such as health information, the majority of respondents had a high sensitivity to privacy protections for such data, while for less sensitive data, consumers were found not to be as concerned. Therefore, consumers do not necessarily place the same level of privacy concerns on all PII, but rather adopt a sliding scale approach, dependent upon the level of sensitivity of the data.

The privacy controls should therefore reflect the proportionality and prioritization required for PII, depending on the sensitivity of the PII at issue. Appendix J briefly references this proportionality approach on page 14, Section DI-1 (Data Quality), Supplemental Guidance. It states, “The measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive PII.” This is one of the few areas in Appendix J where the application or acknowledgement of a proportional approach to different types of PII has been adopted. However, a proportionality approach should be discussed as an overarching theme to all the privacy controls identified in Appendix J, and not be limited to just the data quality privacy control.

Overall, the various privacy controls identified in Appendix J appear to be appropriate for the most sensitive data. For federal agencies that have highly sensitive data, such as social security numbers, it may make sense to apply the full spectrum of controls identified in Appendix J. For other public agencies who may not have such highly sensitive PII, it may be that the respective agency or organization should balance the risks and benefits of adopting such rigorous, thorough privacy controls for non-sensitive PII against resource allocations and availability.

2. Risk Assessment

On page 19, Section AR-2 (Privacy Impact and Risk Assessment), various controls for establishing and conducting risk assessments are discussed. It is recommended that the risk assessment control be emphasized, and provided as a predecessor to all the other privacy controls identified in Appendix J. If an organization identifies the risks and mitigates those risks early on, risks can be prioritized and the appropriate level of subsequent privacy controls to adopt can be strategized. We therefore see the risk assessment as a preparatory step prior to the implementation of the other privacy controls identified in Appendix J.

3. Privacy Policies

On page 4 of Appendix J, Section TR-1 (Privacy Notice), Supplemental Guidance, it states that “Effective notice, **by virtue of its clarity and comprehensiveness**, enables individuals to understand how an organization uses PII generally and, where appropriate to make an informed decision prior to providing PII to an organization.” (emphasis added). In reading this statement, it appears that NIST is advocating an

National Institute of Standards and Technology
Attn: Computer Security Division, Information
September 2, 2011
Page 3

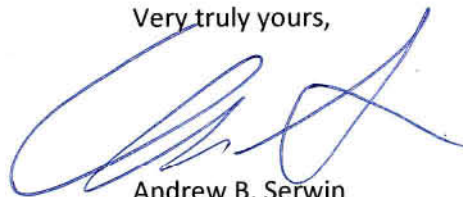
approach to having comprehensive, thorough privacy policies, regardless of the PII at issue. However, it is becoming more generally realized and acknowledged that consumers do not always review privacy policies, but review them in a pattern consistent with certain common consumer agreements. Based on the Lares Institute report, it appears that consumers make active choices about what privacy policies to review. It may be that consumers make value judgments about what they choose to spend their time reviewing, based upon their level of concern and the sensitivity of the data at issue.

The Federal Trade Commission has also expressed skepticism of the effectiveness of comprehensive, long privacy statements. On December 1, 2010, the FTC issued a preliminary report entitled "Protecting Consumer Privacy in an Era of Rapid Change, a Proposed Framework for Businesses and Policymakers." The report calls on companies to improve their privacy policies and notices so that interested parties can compare data practices and choices across companies. The FTC stated that privacy policies will continue to play an important role in promotion of transparency, accountability and competition among companies on privacy issues, but only if the policies are clear, concise and easy to read. Therefore, similar to the proportionality issue discussed above, privacy policies should not necessarily be so comprehensive and thorough in the event the PII at issue is not as sensitive, as it may likely be the case, the consumer will not read it. A concise and clear privacy notice will therefore foster transparency and accountability for organizations in advancing their privacy initiatives.

4. Conclusion

For the most part, Appendix J provides an informative, detailed structure of privacy controls for agencies to adopt in advancing their privacy and security initiatives. However, proportional application of the privacy controls, dependent on the sensitivity of the PII at issue, should be emphasized. Proportional privacy protections places higher restrictions and access barriers on truly sensitive information that either has limited or not use to third-parties and has great capacity to damage individuals, while simultaneously permitting necessary and appropriate access to those having a legitimate need to know certain information, particularly when the information is less sensitive. A proportionality approach to the privacy controls has the advantage of minimizing the societal impact of privacy issues because compliance and resources will be focused on the most appropriate levels of sensitive information.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Andrew B. Serwin", is written over the typed name.

Andrew B. Serwin