Association for Computing Machinery (ACM)
US Public Policy Council of ACM (USACM)

usacm.acm.org
facebook.com/usacm
twitter.com/usacm

The Honorable James R. Clapper
Director of National Intelligence
Office of the Director of National Intelligence
Washington, D.C. 20511

Dear Director Clapper:

In our October 4, 2013 comments to the Review Group on Intelligence and Communications Technologies[1] we recommended an independent systems engineering analysis of data collection and analysis structures, including both intentional and unintentional features. We submit this letter as an expansion of that recommendation and how it could contribute to the President's signals intelligence reform goals. Systems engineering analysis offers a rigorous framework for evaluating the design and operation of complex systems and technologies, including their conformance to policy requirements. Such an approach, for example, could systematically incorporate and highlight relevant tradeoffs across a variety of attributes beyond those related to just immediate functional objectives. This includes risk- risk tradeoffs where attempts to control one risk result in some other, possibly more severe, risk being incurred. A number of the findings of the Review Group as well as the Privacy and Civil Liberties Oversight Board implicate such situations.

We believe this approach can and should play a central role in supporting risk analysis and management as per the Review Group report's Principle 2: "The central task is one of risk management; multiple risks are involved, and all of them must be considered." More specifically, systems engineering analysis could help address:

- Recommendation 18: "[E]stablish a mechanism to monitor the collection and dissemination activities of the Intelligence Community to ensure they are consistent with the determinations of senior policymakers."
- Recommendation 27: "An Office of Technology Assessment should be created within the Civil Liberties and Privacy Protection Board to assess Intelligence Community technology initiatives and support privacy-enhancing technologies..."
- Recommendation 35: "[F]or big data and data-mining programs directed at communications, the US Government should develop Privacy and Civil Liberties Impact Assessments to ensure that such efforts are statistically viable, cost-effective, and protective of privacy and civil liberties."
- Recommendation 36: "[F]or future developments in communications technology, the US should create program-by-program reviews informed by expert technologists, to assess and respond to emerging privacy and civil liberties issues..."

Such an approach could also contribute to:

- Recommendation 6: "[A] study of the legal and policy options for assessing the distinction between meta-data and other types of information."
- Recommendation 20: " [T]he US government should examine the feasibility of creating software that would allow the National Security Agency and other intelligence agencies more easily to conduct targeted information acquisition rather than bulk-data collection."

[1] http://usacm.acm.org/images/documents/ReviewGroupUSACM.pdf

ACM US Public Policy Council (USACM)
1828 L Street NW, Suite 800
Washington, DC 20036

Tel: +1-212-626-0541
Fax: +1-202-667-1066

acmpo@acm.org
usacm.acm.org

We do not address policy issues concerning the scope or legal bases of programs. Also, given the classified nature of these programs, and the incomplete information publicly available, our comments are necessarily high-level. Should you wish further explanation or have follow-up questions, please do not hesitate to contact our Public Policy Office through the contact information at the end of this letter; several of our members have appropriate security clearances.

The objective of systems engineering analysis is to provide an informed basis for understanding the extent to which systems function at the technological level to accomplish their stated goals, including operating in a way that preserves the privacy and civil liberties of the American and foreign publics. Systems engineering analysis relies on sound risk assessment that relates technical characteristics to relevant system risks. Such analysis can establish a technical foundation for evaluating the strength and accuracy of posited properties such as privacy and civil liberties protections.

Beyond an evaluation of current attributes of relevant systems, systems engineering analysis additionally could identify potential improvements that would meet operational goals while more effectively mitigating privacy and civil liberties risks. Such improvements might reduce inadvertent disclosures; improve processes that govern the flow of data; improve assurance that stated policies are actually followed; or improve resistance both to intrusions from external attackers and to abuses by insiders.

In this letter, we outline what would be involved in conducting such analyses. We are happy to provide additional detail if desired. Here we discuss what such an analysis would cover and require as input, how it would be carried out, and how it could address issues of privacy and civil liberties.

Coverage and requirements

Fundamentally, an analysis of informational privacy and related civil liberties is concerned with the flow of data into, through, and out of a system. An elaboration of these elements will provide the structure of the analysis. We suggest using the information life cycle specified in OMB 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, consisting of collection, processing, use, disclosure, retention, and destruction. The goal of the analysis is to describe and analyze the technical architectures governing information flows at each of these stages.

USACM has previously produced a set of privacy recommendations[2] based on generally accepted Fair Information Practice Principles (FIPPs). Based on these principles and relevant quality attributes such as ones drawn from the ISO 25010 standard (and recognizing that the exigencies of the intelligence domain reduce the applicability of certain recommendations, such as those related to consent), we propose that analyses cover the following attributes:

- Auditability (including provenance)—the ability to associate system actions and data with their sources
- Confidentiality—the extent to which the system ensures that data is only accessible for authorized purposes and to those who are authorized
- Integrity—the resistance of data to unauthorized modification

[2] http://usacm.acm.org/privsec/category.cfm?cat=7&Privacy%20and%20Security

ACM US Public Policy Council (USACM)
1828 L Street NW, Suite 800
Washington, DC 20036

Tel: +1-212-626-0541
Fax: +1-202-667-1066

acmpo@acm.org
usacm.acm.org

- Data quality (of both collected and derived data)—the fitness of data for its intended purpose, including its accuracy and currency
- Functional completeness—the extent to which the set of functions addresses all objectives
- Functional correctness—the extent to which the system produces correct results with the necessary degree of precision
- Functional appropriateness—the extent to which the functions achieve objectives

The information requirements for an analysis are a function of the focus on architecture. Understanding the architectures supporting systems at each different information life cycle stage involves analysis of process models (e.g., business process models, UML activity diagrams) and data models (e.g., entity-relationship diagrams, data flow diagrams) as well as logical and physical architecture documentation. Depending on what issues the analysis of these materials identifies, the analysis may require access to greater detail, such as database schemas, interface control documents, or algorithms.

Assessing the distinction between content and meta-data and the implications of that distinction, would be a natural element of such an analysis. In particular, it is important that the risks presented by meta- data are assessed in a technically sound manner, one that considers not just the meta-data in isolation, but how it relates to the attributes above in the context of the analytical techniques applied to it. Systems engineering analysis is useful precisely because it can effectively surface and evaluate these kinds of connections and resultant characteristics.

Similarly, the characteristics of any proposed system for more targeted collection must be analyzed to establish its efficacy in mitigating relevant privacy and civil liberties risks and its potential for introducing new risks and/or worsening existing risks. Technical specifics must be related to larger system attributes that are in turn related to applicable risks.

Carrying out the analysis

While a comprehensive description of the analysis process is beyond the scope of this letter, we highlight some key questions for each of these attributes at each life cycle stage.

Auditability

- What information is captured in audit logs?
- How mutable is the information being tracked?
- Is enough context available to enable detection of policy violations or inappropriate use?

Confidentiality

- What mechanisms enable and what mechanisms prevent confidentiality violations?
- How could personally identifiable information (PII) or other sensitive information leak beyond authorized users for authorized purposes? What failure modes are possible?
- How likely are these failure modes?

Integrity

- On what basis may PII or derived information be altered?
- Can changes be reconstructed to understand and remedy errors or abuses?

Data quality

- What data quality measures are maintained for original PII and derived information? Is

ACM US Public Policy Council (USACM)
1828 L Street NW, Suite 800
Washington, DC 20036

Tel: +1-212-626-0541
Fax: +1-202-667-1066

acmpo@acm.org
usacm.acm.org

provenance tracked?
- How are these quality metrics aligned with purposes?
- What mechanisms support propagation of corrected or otherwise changed information? How does this affect prior targeting decisions?

Functional completeness

- How do functions map to mission objectives, including privacy and civil liberties objectives?
- How much reliance is there on manual processes and for what purposes?

Functional correctness
- What metrics are maintained regarding the reliability of results?
- What are the applicable false positive/negative rates and their acceptability thresholds? How are their values calculated or established?

Functional appropriateness
- Is functionality consistent with stated purposes?
- Under what circumstances is PII pulled versus pushed from a source to a destination?
- What kinds of analyses might be run against the data? To what extent is the availability of this functionality policy dependent?
- Is value from particular functionality commensurate with residual risk? Is externalized risk appropriately accounted for?

Integrating privacy and civil liberties interests

The results of the analysis of these system attributes will carry varying implications for different elements of our privacy recommendations. Further, while the above system attributes were chosen on the basis of USACM's existing privacy recommendations, an analysis will need to consider the implications of its findings for privacy and civil liberties more broadly.

Limitations inherent to FIPPs constrain the issues and risks that can be identified on that basis alone. It is therefore vital that additional frameworks be employed to provide the fullest possible picture of the effects of these systems on privacy and civil liberties. More recent approaches, such as Nissenbaum's contextual integrity heuristic[3] and Solove's taxonomy of privacy problems[4], could be used to interpret the results of systems engineering analyses as they relate to privacy vulnerabilities and impacts. Given the scale, scope, and complexity of the systems involved, it is advisable to complement FIPPs with other approaches.

We appreciate the opportunity to offer these suggestions. Should you have any questions on the above, or need additional information, please contact our Public Policy Office at acmpo@hq.acm.org, or at 212-626-0541.

[3] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life,* Stanford, CA: Stanford University Press, Stanford Law Books, 2010.
[4] Daniel J. Solove, *Understanding Privacy,* Cambridge, MA: Harvard University Press, 2008.

ACM US Public Policy Council (USACM)
1828 L Street NW, Suite 800
Washington, DC 20036

Tel: +1-212-626-0541
Fax: +1-202-667-1066

acmpo@acm.org
usacm.acm.org