HUNTON & WILLIAMS LLP
2200 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, D.C. 20037

TEL 202 • 955 • 1500
FAX 202 • 778 • 2201

FRED H. CATE
EMAIL: FRED@FREDHCATE.ORG

December 12, 2013

Via Email (csfcomments@nist.gov)
Information Technology Laboratory
Attn: Adam Sedgewick
National Institute of Standards and Technology
10 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

RE: Preliminary Cybersecurity Framework Comments

Dear Mr. Sedgewick:

Thank you for the opportunity to submit these comments concerning the Preliminary Cybersecurity Framework, and particularly the Methodology to Protect Privacy and Civil Liberties in Appendix B.

I am a Distinguished Professor and C. Ben Dutton Professor at the Indiana University Maurer School of Law, and director of the Center for Applied Cybersecurity Research, a National Center of Academic Excellence in both Information Assurance Research and Education. I submit these comments today on my own behalf in my role as a senior policy advisor at The Centre for Information Policy Leadership at Hunton & Williams LLP. I have benefitted from broad consultation with my colleagues at, and the members of, the Centre, which, as I believe you know, works to encourage responsible information governance in today's digital society. I alone am responsible for the content of these comments.

I appreciate the significant work that has gone into drafting the Preliminary Cybersecurity Framework, and especially the broad consultations that have been part of the effort to create a framework that is not merely substantively credible, but also practical and capable of implementation. Against that achievement, Appendix B stands in stark relief as an approach to privacy and civil liberties that I fear is neither theoretically sound nor likely to be workable in practice. I summarize briefly below six reasons for this view, before outlining six specific suggestions for improving the protection of privacy within the broader Cybersecurity Framework.

Issues

1. The primary reason for this conclusion is that the proposed privacy methodology is separate from the Preliminary Cybersecurity Framework. Rather than integrate the two so that it is clear from the outset that protecting privacy must be interwoven with cybersecurity, the current document separates them into wholly distinct frameworks. I believe this is a significant error and it sends precisely the wrong signal to those who may implement the Cybersecurity Framework.

2. Another reason for discomfort with Appendix B is that it occurs in a vacuum not only from the Preliminary Cybersecurity Framework, but also from the wide range of successful privacy and data protection programs already implemented by industry leaders. For more than two decades, U.S. industry, in partnership with the Federal Trade Commission (FTC) and other federal, state, and foreign regulators, has been designing, deploying, and refining privacy and data protection programs. Appendix B seems to ignore those entirely, despite the broad requirement of Executive Order 13636, which gave rise to the Preliminary Cybersecurity Framework and which seems to have been followed carefully in the main part of the document, to "incorporate voluntary consensus standards and industry best practices to the fullest extent possible."[1] This point can hardly be overstressed: if you propose as part of the Cybersecurity Framework a privacy methodology that is inconsistent, or incapable of being administered as part of, existing, time-tested industry privacy and data protection programs, then the privacy framework either will be ignored or, if implemented, will impose unnecessary costs without generating additional benefits.

3. Magnifying the concern over the inconsistency of Appendix B is its considerable breadth. It does not appear to be limited to security-related activities to start with, and, even when applied to those activities, it raises the prospect of privacy and civil liberties issues being evaluated where experience shows they are unlikely to exist. Not all aspects of protecting critical infrastructure raise privacy issues—in fact, the vast majority is unlikely to—yet Appendix B proposes a methodology much broader than the likely necessary scope. Moreover, the inclusion of "civil liberties" issues in a framework that primarily targets the private sector is confusing. With very few exceptions, civil liberties are rights or freedoms that apply only in the context of government, not private-sector, activity. Proposing a methodology to protect against

[1] Executive Order 1636 § 7, 78 Fed. Reg. 11739, 11741 (Feb 19, 2013).

private-sector incursions into civil liberties is not only overly broad, but potentially specious.[2]

4. Another problematic aspect of Appendix B is the introductory text suggesting that it is "based on the Fair Information Practice Principles (FIPs) referenced in the Executive Order." FIPs are a poor basis for addressing most cybersecurity privacy issues. In 1998, for example, the FTC, after reviewing the "fair information practice codes" of the United States, Canada, and Europe, reported to Congress that "[t]he most fundamental principle is notice. . . . [because] [w]ithout notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information."[3] The FTC continued, "[t]he second widely-accepted core principle of fair information practice is consumer choice or consent . . . . [over] how any personal information collected from them may be used."[4] U.S. statutes and regulations have tended to parallel the FTC's emphasis on notice and choice. The Obama Administration's 2012 Consumer Privacy Bill of Rights includes as its first principle: "Consumers have a right to exercise control over what personal data companies collect from them and how they use it."[5] Do you really wish to base information assurance programs on notice and choice? While it is true that FIPs are "referenced in the Executive Order," they are referenced in a different section (Section 5) that focuses on the conduct of *government* agencies, not industry, and therefore is unrelated to the development of the privacy and civil liberties methodology addressed in Section 7. Moreover, even in Section 5, the Executive Order refers to FIPs "and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities," making clear that the President is not trying to base everything on FIPs but rather on those "policies, principles, and frameworks" that best apply. I urge you to do the same.

5. The reference to FIPs as the sole basis for the privacy and civil liberties methodology also ignores the extent to which FIPs are being increasingly challenged, precisely because of their often-poor fit in contexts such as big data, ubiquitous surveillance, and

---

[2] Rights articulated in the Constitution generally are protected only against government actions. Only the Thirteenth Amendment, which prohibits slavery, applies directly to private parties. *Clyatt v. United States*, 197 U.S. 207, 216-220 (1905). All other constitutional rights—whether to speak freely, confront accusers, or be tried by a jury of one's peers—regulate the public, but not the private, sector.

[3] U.S. Federal Trade Commission, *Privacy Online: A Report to Congress* 7 (1998), available at http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

[4] *Id.* at 8 (citations omitted).

[5] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation* 47 (2012), available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

cybersecurity.[6] The Expert Group formed by the Organisation for Economic Cooperation and Development (OECD) to review the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted in 1980,[7] the basis for the FIPs, following their 30th anniversary, reached a similar conclusion. While unable to identify any "clear direction . . . as to what changes might be needed at this stage, the Expert Group nevertheless flagged the "role of consent," the "role of the individual," and the "role of purpose specification and use limitation" as warranting "further study."[8] Aspects of the FIPs undoubtedly remain vital and will have application in the context of protecting critical infrastructure, but a rote application of a 33-year-old set of principles is a poor basis for protecting privacy in the 21st century.

6. Whether or not based on FIPs, a number of the requirements of Appendix B go far beyond existing U.S. privacy law. One might argue that as long as compliance with those requirements is voluntary, that should not matter. There are three problems with this argument and therefore with the inconsistency of Appendix B. The first is that many people believe—and the entire context of the Executive Order and the Preliminary Cybersecurity Framework suggests—that the requirements may not be voluntary for long, or may be voluntary only as long as they are widely followed. The second is that the Preliminary Cybersecurity Framework is likely to have a significant signaling function, indicating to foreign governments and international organizations the direction that the U.S. government believes cybersecurity and privacy regulation should take. The third is that the inconsistency of Appendix B with existing law heightens the inconsistency between this framework and the data protection programs already in place to ensure accountability for the responsible stewardship of personal data under existing law.

---

[6] *See* Fred H. Cate & Viktor Mayer-Schönberger, *Data Use and Impact Global Workshop* (2013), available at http://cacr.iu.edu/sites/cacr.iu.edu/files/Use_Workshop_Report.pdf; Fred H. Cate, Peter Cullen & Viktor Mayer-Schönberger, *Data Protection Principles for the 21st Century* (2013), available at http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf.

[7] O.E.C.D. Doc. (C 58 final) (Oct. 1, 1980), available at http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html.

[8] OECD, "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines," OECD Digital Economy Papers No 229, 6-9 (2013), available at http://www.oecd-ilibrary.org/docserver/download/5k3xz5zmj2mx.pdf?expires=1385481986&id=id&accname=guest&checksum=7F674964BA2D22F1277B4F7324E25ED7.

Recommendations

To address these concerns, I encourage you to consider the following:

1. Eliminate Appendix B and move privacy protection into Appendix A, so that the protection of privacy is clearly integrated with cybersecurity. The "Functions" and "Categories" in Appendix A for which there are privacy considerations should contain new points to address those considerations.

2. Make explicit that the privacy protections apply only in the context of information assurance activities. This will help focus attention and eliminate concerns that the document is an end-run around existing FTC and congressional efforts to address broader privacy issues.

3. Limit the privacy methodology, wherever it appears, to objectives and principles, rather than specific tasks. In addition, limit the methodology to privacy—not other civil liberties—or if the protection of other civil liberties is to be included, clarify that this responsibility can apply only to government entities. These changes are more consistent with a "methodology," they reduces the likelihood of inconsistency with existing privacy laws, they increase the likelihood that established businesses that own and operate the majority of critical infrastructure will be able to implement privacy protections within existing privacy and data protection programs, and they reduce the chance of weakening the government's obligation to protect civil liberties by trying to extend it to the private sector.

4. Eliminate any reference to FIPs. It is unnecessary and largely misleading because the FIPs that the FTC considers "most fundamental" are unlikely to apply in the cybersecurity context in any event. Furthermore, it suggests that the privacy methodology is outdated.

5. Focus instead on more relevant principles of "accountability" and "stewardship" of personal data. These 21st-century principles increasingly serve as the foundation of successful industry privacy and data protection programs; reflect a commitment to the appropriate, responsible, risk-based use of personal data that is more consistent with the Preliminary Cybersecurity Framework; and provide more meaningful protection for personal data. The Centre, in partnership with member companies and data protection

regulators, has developed a number of documents developing the accountability approach to data protection; I urge you to consult them.[9]

6. Do not assume that all, or even most, information assurance activities will raise privacy issues. Though some important privacy issues may be raised here, such as sharing personally identifiable information (PII) with the government, those are not the norm. Moreover, given recent revelations about the federal government's existing extraordinary access to personal data, even those critical issues—most of which involve government access to data—are going to be difficult to address meaningfully. It seems counterproductive and runs the risk of calling the entire Cybersecurity Framework into question if the Framework purports to create significant burdens on industry before sharing cyber threat information with the government that might contain PII if the government already has access to the data.

My colleagues at the Centre and I stand ready to provide any additional information or assistance in drafting specific language that you might wish. In the meantime, thank you again for the opportunity to submit these comments.

Sincerely,

Fred H. Cate
Senior Policy Advisor

[9] *See, e.g.*, http://www.informationpolicycentre.com/accountability-based_privacy_governance/.