iapp
international association
of privacy professionals

December 12, 2013

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

RE: Preliminary Cybersecurity Framework Comments – Privacy Methodology

Dear Mr. Sedgewick,

The International Association of Privacy Professionals (IAPP) is pleased to submit comments to the consultation on a preliminary version of the Cybersecurity Framework (Cybersecurity Framework) developed by the National Institute of Standards and Technology (NIST) in response to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." The IAPP does not opine on the necessity or soundness of integrating privacy rules into the Cybersecurity Framework either as a separate appendix (as currently structured in Appendix B: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program (Privacy Methodology)) or as an integral component of Appendix A: Framework Core (Framework Core). Instead, assuming that privacy is ultimately addressed in the Cybersecurity Framework, IAPP proposes that the *personnel who are designated "to implement and provide oversight for privacy policies and practices designed to minimize the impact of cybersecurity activities on privacy and civil liberties" be duly qualified, adequately trained and certified privacy professionals.*

A privacy workforce

Section C.4 of Appendix C of the Cybersecurity Framework states: "A skilled cybersecurity workforce is necessary to meet the unique cybersecurity needs of critical infrastructure." The IAPP posits that duly qualified professionals are similarly required in the context of privacy implementation.

The NIST explains that "[w]hile it is widely known that there is a shortage of general cybersecurity experts, there is also a shortage of qualified cybersecurity experts with an understanding of the specific challenges posed to critical infrastructure. As the critical infrastructure threat and technology landscape evolves, the cybersecurity workforce must continue to adapt to design, develop, implement, maintain and continuously improve the necessary practices within critical infrastructure environments." Moreover, the NIST suggests

that "[w]hile progress has been made through [various] programs, greater attention is needed to help organizations understand their current and future cybersecurity workforce needs, and to develop hiring, acquisition, and training resources to raise the level of technical competence of those who build, operate, and defend systems delivering critical infrastructure services."

These very needs are also manifest in the context of the privacy workforce, which deals with issues of great legal, policy, technological and financial consequence to businesses and government organizations. Through training and certification, continuing education, professional conferences, a research center and multiple publication outlets, the IAPP delivers the privacy workforce with the requisite tools and resources to serve these needs.

The past decade has seen the emergence of a privacy workforce combining skills, qualifications and responsibilities from the fields of law, public policy, technology and business organization. In their article "Privacy on the Books and on the Ground," Kenneth Bamberger and Deirdre Mulligan stress, "the importance of the professionalization of privacy officers as a force for transmission of consumer expectation notions of privacy from diverse external stakeholders, and related 'best practices', between firms."[1]

Chief privacy officers (CPOs) began to emerge in the U.S. in the 1990s.[2] The role developed first in the financial services and health sectors, gradually expanding to additional industries. Harriet Pearson became the first CPO of a Fortune 100 company, IBM, in November 2000.[3]

The information, training, and networking needs of these newly appointed professionals were met by two new trade associations, the Privacy Officers Association (POA) and the Association of Corporate Privacy Officers (ACPO), which was created by Professor Alan Westin in 2000. In 2001, these groups merged under a new name, the International Association of Privacy Officers (IAPO), which held its first "Privacy and Data Protection Summit" in Arlington, Virginia in May 2001. In 2003, the IAPO, which had a few hundred members, changed its name to the IAPP. In 2003, the IAPP had 1,000 members. It debuted a certification program in corporate privacy compliance, the Certified Information Privacy Professional (CIPP), and held its first exam in 2004.

Today, IAPP has more than 14,000 members, coming from government, academia and civil society, in 80 countries around the world. More than 6,000 members have been certified under the CIPP program, which has branched out to feature specializations in US (CIPP/US), EU (CIPP/E), Canada (CIPP/C), U.S. government (CIPP/G) and IT (CIPP/IT).

---

[1] Kenneth Bamberger and Deirdre Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2010).

[2] Jennifer Glasgow was named leader of Acxiom's privacy efforts in 1991. *See* Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, ___ OHIO ST. L. J. (forthcoming 2014).

[3] *See, e.g.*, Linda Rosencrance, *IBM Joins Chief Privacy Officer Trend*, COMPUTERWORLD, (Nov. 30, 2000), http://www.computerworld.com/s/article/54492/IBM_joins_chief_privacy_officer_trend?pageNumber=1

This year, IAPP launched the Certified Information Privacy Manager (CIPM) program. While the CIPP program covers the "what" of privacy law, the CIPM adds an additional layer addressing the "how" of privacy– *i.e.*, describing the business management practices that allow organizations to give life to privacy standards. As such, it tracks the evolution of the privacy profession from a technical, legal compliance role into a strategic organizational and management function. Aimed at chief privacy officers, corporate privacy managers, compliance officers, risk managers, information security and auditing professionals and a host of others with responsibility for implementing privacy policy, the CIPM covers subject matter like creating a company vision, structuring a privacy team, measuring performance and developing and implementing a privacy program framework. It demonstrates an understanding of privacy program governance and the skills necessary to establish, maintain and manage a privacy program across all stages of its operational life cycle.

In addition to certification, the IAPP offers a wide range of educational and professional conferences (the annual Global Privacy Summit now draws more than 2,500 participants; the Europe Data Protection Congress is the largest privacy conference in Europe); networking opportunities (there are currently more than 50 local Knowledgenet chapters spread across 20 countries); multiple publications (including the Daily Dashboard, which reaches 25,000 subscribers); and a newly formed research center named after Professor Westin (offering two fully funded annual scholarships to graduate students and overseen by the IAPP VP of Research and Education).

To be a member of the privacy workforce today means more than just being tasked by an HR or IT manager to "do privacy". It entails becoming steeped in a growing interdisciplinary body of knowledge, and maintaining a firm grasp of new developments in technology, business and law.

Qualified privacy professionals should deploy the Privacy Methodology

In an increasing number of organizations, privacy professionals oversee business-critical data management functions. Data have become a raw material of production, an asset class of great value, as well as a source of operational and regulatory risk. Just as qualified civil engineers build bridges and certified dentists perform root canals, so too should data management be entrusted to duly qualified, adequately trained and certified privacy professionals.

Qualification and training requirements are already mandated by regulators in the realm of data security. In a line of decisions dating back to 2004, the Federal Trade Commission (FTC) required parties in consent decrees to undergo periodic assessments by "a person qualified as a Certified Information System Security Professional (CISSP); a person qualified as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security Institute (SANS); or by a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission."[4] In a recent case involving alleged privacy violations, the

[4] See, e.g., In the Matter of MTS (Tower Records), May 28, 2004, http://www.ftc.gov/os/caselist/0323209/040602do0323209.pdf; In the Matter of Nationwide Mortgage

FTC mandated that defendant, application developer Path, conduct periodic privacy assessments "[to] be prepared ... by a person that has a minimum of three (3) years of experience in the field of privacy and data protection."[5]

The consolidated version of the draft European General Data Protection Regulation, which was recently submitted by the Committee on Civil Liberties, Justice and Home Affairs for Parliament vote, mandates a specific set of skills and qualifications for data protection (*i.e.*, privacy) officers. Under Recital 75a of the consolidated version, "[t]he data protection officer should have at least the following qualifications: extensive knowledge of the substance and application of data protection law, including technical and organizational measures and procedures; mastery of technical requirements for privacy by design, privacy by default and data security; industry-specific knowledge in accordance with the size of the controller or processor and the sensitivity of the data to be processed; the ability to carry out inspections, consultation, documentation, and log file analysis; and the ability to work with employee representation. The controller should enable the data protection officer to take part in advanced training measures to maintain the specialized knowledge required to perform his or her duties. The designation as a data protection officer does not necessarily require fulltime occupation of the respective employee."

While "Awareness and Training" are addressed in the Cybersecurity Framework both in the Framework Core and in the Privacy Methodology, the requirements for the privacy workforce fall short of those ascribed to cybersecurity professionals. The Framework Core requires an "organization's personnel and partners [to be] adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements." The Privacy Methodology requires senior executives to "assign responsibility to designated personnel to implement and provide oversight for privacy policies and practices designed to minimize the impact of cybersecurity activities on privacy and civil liberties. Have regular training for employees and contractors on following such policies and practices." Hence, the current focus is on privacy training for the general workforce as opposed to credentials and qualifications required for those deploying the Privacy Methodology itself.

Sound data management practices are not common knowledge. They require laborious training, continuous education, and a verifiable method of certifying skills. IAPP does not seek exclusivity

---

Group, April 12, 2005, http://www.ftc.gov/os/adjpro/d9319/050415dod9319.pdf; In the Matter of Nations Title Agency, June 19, 2006, http://www.ftc.gov/os/caselist/0523117/0523117NationsTitleDecisionandOrder.pdf; United States of America (for the Federal Trade Commission) v. American United Mortgage Company, December 17, 2007, http://www.ftc.gov/os/caselist/0623103/071217americanunitedmrtgstipfinal.pdf; In the Matter of Goal Financial, April 9, 2008, http://www.ftc.gov/os/caselist/0723013/080415decision.pdf; In the Matter of Genica Corporation, March 16, 2009, http://www.ftc.gov/os/caselist/0823113/090320genicado.pdf; In the Matter of Dave & Buster's, May 20, 2012, http://www.ftc.gov/os/caselist/0823153/100608davebustersdo.pdf; In the Matter of SettlementOne Credit Corporation, August 17, 2011, http://ftc.gov/os/caselist/0823208/110819settlementonedo.pdf; In the Matter of EPN, Inc., October 3, 2012, http://www.ftc.gov/os/caselist/1123143/121026epndo.pdf; In the Matter of Compete, February 20, 2013, http://ftc.gov/os/caselist/1023155/130222competedo.pdf.

[5] United States of America (for the Federal Trade Commission) v. Path, Inc., February 8, 2013, http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf.

as a source of privacy knowledge, training and certification. Competing programs exist, and more will be created as the privacy workforce rapidly grows. Consequently, IAPP proposes requiring individuals who are tasked with deploying the Privacy Methodology to be *adequately trained and duly certified, for example by programs such as the CIPP and CIPM.*

We remain at your disposal for any questions or comments.
Omer Tene

Vice President of Research and Development