



international association  
of privacy professionals

October 16, 2014

National Privacy Research Strategy  
NCO, Suite II-405, 4201 Wilson Blvd.  
Arlington, VA 22230

To whom it may concern,

The International Association of Privacy Professionals (IAPP) respectfully submits these comments in response to the National Science Foundation (NSF) Request for Information (RFI) on a National Privacy Research Strategy (NPRS). The IAPP commends the decision of the White House Office of Science and Technology Policy to develop a NPRS, and recommends to the NSF to expand the scope of its initiative beyond theoretical research of privacy concepts into practical analysis of their implementation on the ground. Specifically, as privacy emerges as a new profession, dealing with cutting edge ethical and scientific issues at the cusp of technological innovation, efforts should be invested (a) to create a privacy body of knowledge to train new professionals on the ground; and (b) to explore organizational mechanisms to introduce privacy and data ethics into corporate decision making processes.

### **Privacy theory; privacy practice**

Much like law, privacy is not a purely philosophical, theoretical construct. It is an emergent profession requiring skills from fields as diverse as public policy, law, economics, sociology, IT and computer science. It involves a delicate balance among divergent interests and a careful deliberation of issues that emerge as new technologies grate against established social norms. In their article *Privacy on the Books and on the Ground*, Kenneth Bamberger and Deirdre Mulligan recognized, “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.”<sup>1</sup>

Consider, for example, the ongoing debate around anonymization or de-identification.<sup>2</sup> Once viewed as a silver bullet, allowing organizations to reap the benefits of data without bearing

---

<sup>1</sup> Kenneth Bamberger and Deirdre Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2010).

<sup>2</sup> Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).



international association  
of privacy professionals

privacy costs, de-identification has been discounted by computer scientists and statisticians, who have shown that with sufficient interest and effort, apparently de-identified data can readily be re-identified.<sup>3</sup> Other computer scientists have devised more robust mechanisms to allow privacy-protective data use, such as differential privacy.<sup>4</sup> But even as the theoretic debate rages in mathematics and computer science departments at Harvard and MIT, professionals on the ground continue to implement “pretty good” de-identification, including not only technical but also contractual and organizational tools, to reduce, even if not eliminate, privacy risks.<sup>5</sup> In its 2012 Report, *Protecting Consumer Privacy in an Era of Rapid Change*, the Federal Trade Commission sanctioned this practical approach, stating that it would view “data [as] not ‘reasonably linkable’ to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data.”<sup>6</sup>

Hence, while the theory and science of de-identification advance, practical de-identification methods, already implemented on the ground and allowing organizations to unleash the tremendous benefits of data analysis, should follow suit in lockstep.

### **An emerging profession**

For more than a decade, the IAPP has laid the groundwork for professionalization of the privacy world, setting the parameters for the development of a privacy workforce, including chief privacy officers (CPOs) and their staff.<sup>7</sup> It currently provides training, certification, conferences, publications, professional resources and industry research to more than 18,000 members in more than 100 countries around the world. The IAPP believes that employees who are designated to implement and provide oversight for data governance in organizations should be duly qualified, adequately trained and certified professionals. Consequently, it has developed,

---

<sup>3</sup> See, e.g., Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, in PROCEEDINGS OF THE 2008 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 111, 111-12 (May 19, 2008), available at <http://www.senyt.dk/bilag/netflix2.pdf>.

<sup>4</sup> Cynthia Dwork, *Differential Privacy*, 2006 INT’L COLLOQUIUM ON AUTOMATA, LANGUAGES AND PROGRAMMING pt. II, at 8, [http://www.dbis.informatik.hu-berlin.de/fileadmin/lectures/SS2011/VL\\_Privacy/Differential\\_Privacy.pdf](http://www.dbis.informatik.hu-berlin.de/fileadmin/lectures/SS2011/VL_Privacy/Differential_Privacy.pdf).

<sup>5</sup> Ann Cavoukian & Khaled El Emam, *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy*, June 2011, <http://www.ipc.on.ca/images/Resources/anonymization.pdf>.

<sup>6</sup> Federal Trade Commission, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, 36-40 (2012), <http://ftc.gov/os/2012/03/120326privacyreport.pdf>.

<sup>7</sup> Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, 74 OHIO ST. L. J. 897 (2013).



international association  
of privacy professionals

and continues to invest in, a comprehensive body of knowledge for training and certifying the individuals who implement privacy policies on the ground.

More than 7,000 members have already been trained and certified under the IAPP's Certified Information Privacy Professional (CIPP) program, which has branched out to feature specializations in US (CIPP/US), EU (CIPP/E), Canada (CIPP/C) and U.S. government (CIPP/G). Over the past year, the IAPP launched the Certified Information Privacy Manager (CIPM) program, which presents professionals with the business management practices that allow organizations to operationalize privacy standards on the ground; and the Certified Information Privacy Technologist (CIPT) program, which trains technologists who are charged with securing data privacy at all stages of IT product and service lifecycles.

In addition to certification, the IAPP offers a wide range of educational and professional conferences (the annual Global Privacy Summit now draws around 3,000 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 30,000 subscribers); and a newly formed research center named after privacy pioneer Professor Alan Westin (offering two fully funded annual scholarships to graduate students and overseen by the IAPP VP of Research and Education).

These initiatives help define, support and improve the privacy profession, and consequently deliver better privacy results to individuals.

### **Privacy today; privacy in the future**

To "own" privacy and data protection within an organization 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. Sound data management practices are not common knowledge. They require laborious training, continuous education, and a verifiable method of certifying skills. 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.



international association  
of privacy professionals

Indeed, over the past few years it has become clear that when it comes to privacy, even legal compliance and sound security practices are not sufficient to meet consumer expectations.<sup>8</sup> With companies becoming laboratories for big data research, data ethics have become a critical component of a privacy framework. Companies cannot view privacy as a compliance matter to be addressed by legal departments or a technical issue handled by IT. Rather, to avert public embarrassment and consumer backlash, they must set up ethical review processes and instill issue-spotting skills in employees throughout the organization.

This new trajectory requires additional investment in developing substantive and procedural safeguards for the still nascent field of data ethics.

### **A research agenda**

A NPRS should comprise not only theoretical research into privacy concepts but also practical analysis of their implementation on the ground. Bamberger and Mulligan note: “our account underscores the importance of empirical inquiry and thick institutional engagement in considering contested issues of regulatory strategy, technological complexity, social and institutional networks, and the protection of individual and communal interests in the private sphere. If privacy is to be protected in an increasingly connected world, debates over its formal regulation must increasingly be informed by the ways that today’s frameworks operate on the ground.”<sup>9</sup>

Policymakers would benefit from an examination of a range of current ways that companies are using CPOS and their staff, advisory boards, internal committees, and accountability processes to address ethical, legal and policy issues. Research into the integration of privacy into corporate governance mechanisms would draw on the practices of existing organizations as well as processes put in place in academic, health and research institutions. It would set forth parameters for new institutional mechanisms, including the necessary skills, reporting structure, areas of responsibility and compensation schemes as well as concerns about diversity, accountability and fair representation.

In addition, the privacy bodies of knowledge should be expanded and deepened, with modules created for professionals in specific fields, such as education, healthcare, finance and retail. They should be distributed to a growing number of professionals within organizations, including

---

<sup>8</sup> J. Trevor Hughes & Omer Tene, *The Truth Is Out There: Compliance and Security Are Not Enough*, *Privacy Perspectives*, October 3, 2014, <https://privacyassociation.org/news/a/the-truth-is-out-there-for-big-data-privacy-compliance-and-security-are-not-enough>.

<sup>9</sup> Bamberger & Mulligan, *supra* note 1, at 315.



international association  
of privacy professionals

not only members of compliance departments and IT teams, but also other employees throughout an organization who handle individuals' data.

The IAPP remains ready to provide input to the NPRS and help harness the knowledge of thousands of professionals all over the world to the Administration's research initiative.

Sincerely yours,

A handwritten signature in blue ink that reads 'J. Trevor Hughes'.

J. Trevor Hughes, CIPP  
President & CEO  
IAPP

A handwritten signature in blue ink that reads 'Dr. Omer Tene'.

Dr. Omer Tene  
VP Research and Education  
IAPP