

August 20, 2018

## Before the Federal Trade Commission

### **In re: FTC Hearings on Competition and Consumer Protection in the 21<sup>st</sup> Century**

Topic 5: The Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters

The International Association of Privacy Professionals (IAPP) respectfully submits its comments to the Federal Trade Commission's Hearings on Competition and Consumer Protection in the 21<sup>st</sup> Century. The IAPP submits that in addition to considering privacy policies, rules and regulations, the FTC should recognize professionalization as a major tool for the promotion of improved data governance practices and privacy programs in organizations.

At an age when personal data has become a central raw material for production underlying new business models and driving research and innovation, managing personal data in organizations has become a profession with a full-fledged body of knowledge that includes legal, technical and management components. The role of Chief Privacy Officers (CPOs) has grown to a senior C-suite office in thousands of businesses, including not only Fortune 500 companies but also SMEs, across all industry sectors. In data intensive industries, such as technology and finance, privacy offices comprise dozens and even hundreds of privacy professionals. Under Europe's new General Data Protection Regulation (GDPR), a large swath of industry – not only in Europe but often in the US – is now required to appoint Data Protection Officers (DPOs).

The past two decades have seen the emergence of a privacy workforce combining skills, qualifications and responsibilities from the fields of law, public policy, technology and business management. In their book *Privacy on the Ground*, Kenneth Bamberger and Deirdre Mulligan stressed, "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>

---

<sup>1</sup> Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (1st edn, 2015).

#### **Global Headquarters**

Pease International Tradeport  
75 Rochester Ave.  
Portsmouth, NH 03801 USA  
Tel: +1 603.427.9200 | 800.266.6501  
iapp.org

#### **European Office**

Rue du Luxembourg 22  
1000 Brussels, Belgium  
Tel: +32.(0)2.761.66.86  
europe@iapp.org

Accordingly, data management should no longer be regarded as a role that employees in legal or HR departments fulfil off the side of their desk. Rather, it is a new profession with standards, best practices and norms. Responsible practices for personal data management are not common knowledge. They require training, continuous education, and verifiable methods for identifying and recognizing a common knowledge base. Put simply, the digital economy needs privacy professionals. Requiring organizations to implement internal governance programs that deploy such professionals will ensure higher professional standards and more responsible data uses.

## The accountability principle

The concept of accountability stems from the 1980 Organization for Economic Cooperation and Development (OECD) Privacy Guidelines,<sup>2</sup> the first international effort to create a unified privacy framework. Under the OECD's accountability principle, "a data controller should be accountable for complying with measures which give effect to the principles stated above".<sup>3</sup> As further explained in the 2013 revisions to the OECD Guidelines, accountability means putting in place a privacy management program that is appropriate to the risks of an operation, provides for internal oversight and governance, includes plans for responding to inquiries and incidents, and is continuously updated and reviewed.<sup>4</sup> In Europe, the GDPR for the first time formally introduced the concept of accountability into EU law, both as an explicit principle<sup>5</sup> and encoded in provisions throughout the Regulation. The GDPR requires controllers to "implement technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation".<sup>6</sup>

In the US, even in the absence of formal legislation, accountability measures have emerged as a mainstay of companies' efforts to protect brand reputation, respect consumer expectations, and reduce risks associated with the surge in collection and use of personal data. Over the past two decades, the FTC has entered into more than 150 settlement orders in enforcement actions against consumer deception and unfairness focused on privacy and data security against companies across a plethora of industry sectors.<sup>7</sup> Although not an explicit feature of the FTC Act, which dates back more than a century, the agency depicted accountability as "embodied in the FTC's

<sup>2</sup> Org. for Econ. Co-operation & Dev. [OECD], Council Recommendation Concerning Guidelines Governing the Protection of Privacy ! and Transborder Flows of Personal Data, OECD Doc. C(80)(58) Final (1 October 1980). !

<sup>3</sup> Id. at art. 14. !

<sup>4</sup> Org. for Econ. Co-operation & Dev. [OECD], Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), at art. 15. !

<sup>5</sup> Article 5(2): 'The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')'. !

<sup>6</sup> Article 24(1). !

<sup>7</sup> Chris Jay Hoofnagle, Federal Trade Commission Privacy Law and Policy (1st edn, 2016). !

### Global Headquarters

Pease International Tradeport  
75 Rochester Ave.  
Portsmouth, NH 03801 USA  
Tel: +1 603.427.9200 | 800.266.6501  
iapp.org

### European Office

Rue du Luxembourg 22  
1000 Brussels, Belgium  
Tel: +32.(0)2.761.66.86  
europe@iapp.org

framework”.<sup>8</sup> Importantly, in dozens of enforcement actions in the field of privacy and data security, the FTC ordered companies to set up elaborate accountability programs for data governance, including external third party audits for periods up to twenty years.

In 2012, the Administration’s proposed Consumer Privacy Bill of Rights included explicit accountability measures,<sup>9</sup> as did amendments to the Health Insurance Portability and Accountability Act (HIPAA) in 2013, including mandatory investigations of possible violations and penalties even for inadvertent violations in the health sector.<sup>10</sup>

An important accountability mechanism is the requirement to conduct privacy impact assessments (PIAs) for high risk processing activities. PIAs have their origins in guidelines issued by the US Health, Education and Wellness (HEW) department in 1973. Since then, they have been adopted in guidance issued by privacy commissioners from Australia, Canada, Hong Kong and New Zealand in the mid-1990s.<sup>11</sup> In the GDPR, the PIA requirement is part of a broader mandate that includes appointing a Data Protection Officer to promote privacy governance within organizations that engage in risky processing (Article 37(1)). These efforts build off the experiences of privacy management programs among US companies and aim to narrow the gap between privacy protections on the books and on the ground.<sup>12</sup>

## A profession emerges

In its enforcement actions in the field of data security, the FTC required companies to demonstrate accountability by employing qualified professional specialists. For example, in the *Fandango and Credit Karma* cases, the agency called for:

“reports (‘Assessments’) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such

---

<sup>8</sup> FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012). !

<sup>9</sup> The White House, Consumer Data in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (February 2012). !

<sup>10</sup> 45 CFR Parts 160 and 164, “Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act”. !

<sup>11</sup> David Tancock, Siani Pearson and Andrew Charlesworth, The Emergence of Privacy Impact Assessments, HP Laboratories (21 May 2010). !

<sup>12</sup> Kenneth A. Bamberger and Deirdre K. Mulligan, Privacy on the Books and on the Ground, 63 Stan. L. Rev. 247 (2011). !

### Global Headquarters

Pease International Tradeport  
75 Rochester Ave.  
Portsmouth, NH 03801 USA  
Tel: +1 603.427.9200 | 800.266.6501  
iapp.org

### European Office

Rue du Luxembourg 22  
1000 Brussels, Belgium  
Tel: +32.(0)2.761.66.86  
europe@iapp.org

Assessments shall be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience in secure mobile programming; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and secure mobile programming; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection.”<sup>13</sup>

Similarly, the agency should recognize that in order to bind companies to their privacy commitments—which include deployment of complex measures of data inventory, data mapping, consent management, de-identification, encryption and security—it should require them to demonstrate accountability by hiring and deploying duly qualified privacy professionals. The promises and commitments in privacy consent decrees would be hollow without a privacy profession to implement them into the day to day activities of companies.

The concept of an internal privacy officer has risen to prominence as a central feature under the US approach to privacy protection. In the late 1990s, with the growth of information technology, an emphasis on enhancing trust in the nascent digital economy forced companies to devote internal resources toward protecting consumer expectations. Companies that failed to satisfactorily address the public’s privacy concerns—such as Eli Lilly, which mistakenly revealed the email addresses of hundreds of Prozac patients,<sup>14</sup> or DoubleClick, which proposed to combine clickstream data with offline personally identifying information<sup>15</sup>—were met with public scorn.

The role of the CPO appeared in response, with companies creating internal positions for privacy specialists. In the decade that followed, an entire industry emerged focused on managing privacy risks and creating accountable data governance measures. The IAPP, born in 2000 to serve the small, but budding privacy profession, grew to ten thousand members in 2012 and more than 43,000 in 2018. The privacy profession is built upon the bedrock principle of accountability – that the success of privacy protection depends not on the vindication of formulaic notice and consent but rather on securing the trust of those whose information is at stake through responsible data practices.<sup>16</sup>

US-based CPOs are often executives and C-level officers, reflecting a perception within firms of data as a strategic asset and privacy as a core function inherent in establishing consumer trust and brand reputation.

---

<sup>13</sup> FTC Press Release, Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Failing to Securely Transmit Sensitive Personal Information (March 28, 2014). !

<sup>14</sup> FTC Press Release, Eli Lilly Settles FTC Charges Concerning Security Breach (January 18, 2002). !

<sup>15</sup> Andrea Petersen, DoubleClick Reverses Course After Outcry on Privacy Issue, Wall Street Journal (3 March 2000). !

<sup>16</sup> Andrew Clearwater and J. Trevor Hughes, In the Beginning . . . An Early History of the Privacy Profession, 74 Ohio St. L.J. 897 ! (2013). !

#### Global Headquarters

Pease International Tradeport  
75 Rochester Ave.  
Portsmouth, NH 03801 USA  
Tel: +1 603.427.9200 | 800.266.6501  
iapp.org

#### European Office

Rue du Luxembourg 22  
1000 Brussels, Belgium  
Tel: +32.(0)2.761.66.86  
europe@iapp.org

While their responsibilities vary from firm to firm, most CPOs are responsible for implementing privacy management programs that include conducting PIAs, auditing company practices, managing data flows and training employees, in addition to monitoring compliance. Increasingly, CPOs are involved in product design and engineering processes. By 2015, according to a joint study by the IAPP and EY, US companies, on average, had larger privacy budgets and greater staff resources than their European counterparts.<sup>17</sup>

The role of the data protection officer (DPO) outlined in the GDPR takes elements from both the EU and US models. Like under German law, DPOs will be mandatory for public authorities and for a subset of companies – those that process sensitive data on a large scale or that conduct “regular and systematic monitoring of data subjects on a large scale”.<sup>18</sup> But, like the US CPO, the DPO’s role will extend beyond monitoring compliance and record-keeping to include strategic planning, employee training, auditing, advising on PIAs, and interacting with supervisory authorities.<sup>19</sup> With GDPR, EU based DPOs will potentially elevate to a level commensurate with their US counterparts.

## A professional association

A not for profit, non-policy professional association, the IAPP has worked to define, support and improve the privacy profession globally. The IAPP has developed and launched the only globally recognized, ISO/ANSI accredited, credentialing programs in information privacy: the Certified Information Privacy Professional (CIPP), the Certified Information Privacy Manager (CIPM) and the Certified Information Privacy Technologist (CIPT). The CIPP, CIPM and CIPT are the leading privacy certifications for more than 10,000 professionals around the world who serve the data protection, information auditing, information security, legal compliance and/or risk management needs of their organizations.

In addition, the IAPP offers a full suite of educational and professional development services and holds annual conferences that are recognized internationally as the leading forums for the discussion and debate of issues related to privacy policy and practice. The annual Global Privacy Summit now draws more than 4,000 participants; the Europe Data Protection Congress is the largest privacy conference in Europe with more than 2,000 attendees. With more than 120 local KnowledgeNet chapters in more than 50 countries, the IAPP provides daily networking and continuing education opportunities for thousands of privacy professionals across the globe.

---

<sup>17</sup> IAPP-EY Annual Privacy Governance Report 2015. !

<sup>18</sup> Article 37(1). !

<sup>19</sup> Article 39. !

### Global Headquarters

Pease International Tradeport  
75 Rochester Ave.  
Portsmouth, NH 03801 USA  
Tel: +1 603.427.9200 | 800.266.6501  
iapp.org

### European Office

Rue du Luxembourg 22  
1000 Brussels, Belgium  
Tel: +32.(0)2.761.66.86  
europe@iapp.org

Together with leading graduate programs in law, computer science and business, in the US and abroad, the IAPP established the Privacy Pathways program, intended to serve as an on ramp to the profession for students who take a group of courses in privacy, complete an externship or an internship and pass a certification exam.

The IAPP's sections, the Privacy Law Bar and the Privacy Engineering Forum, convene professionals from these respective disciplines to advance knowledge and share best practices. This year, the American Bar Association (ABA) accredited the IAPP to certify lawyers in the specialty area of Privacy Law. This means that US attorneys who meet the IAPP's specialist designation requirements are permitted under the professional responsibility rules of more than 25 states to advertise their specialization in privacy law. To obtain the designation, an attorney must be admitted in good standing in at least one US state; hold a CIPP/US as well as either a CIPM or CIPT designation; pass a special Ethics Exam administered by the IAPP (or submit a recent MPRE score of 80+); provide proof of "ongoing and substantial" involvement practicing privacy law; supply evidence of continuing education in privacy law; and provide at least five peer references from attorneys, clients or judges.

## Conclusion

To ensure that privacy policies do not remain on the books but are also implemented on the ground, the IAPP is working to define, support and improve the privacy profession globally. The FTC can support this mission by recognizing the importance and value of privacy qualifications, training, education and best practices as an integral part of an ecosystem that promotes technological innovation while maintaining responsible data practices.

Respectfully Yours,

Omer Tene  
Vice President, Chief Knowledge Officer

### Global Headquarters

Pease International Tradeport  
75 Rochester Ave.  
Portsmouth, NH 03801 USA  
Tel: +1 603.427.9200 | 800.266.6501  
iapp.org

### European Office

Rue du Luxembourg 22  
1000 Brussels, Belgium  
Tel: +32.(0)2.761.66.86  
europe@iapp.org