IEEE
Advancing Technology for Humanity

IEEE POSITION STATEMENT

In Support of Privacy Engineering

Adopted by the
IEEE Board of Directors

18 November 2018

IEEE endorses the emerging field of Privacy Engineering, which is the use of engineering knowledge and techniques to systematically address risks associated with planned and authorized functioning of systems that collect, use and disclose personal information.[1] Privacy Engineering has been described as "the discipline of understanding how to include privacy as a non-functional requirement in system engineering."[2] [3]

Personal data has become increasingly important in the development of new products and services, improvement of existing products and services, and the creation of social and economic value.[4] As a result, technologists are increasingly expected to build and maintain systems that meet technical requirements, and at the same time respect individual expectations of privacy and comply with data protection standards in different domains (such as health, energy, transportation, social computing, law enforcement, and public services), on different infrastructures and architectures (such as cloud, grid,

[1] While privacy has historically been a concept applied to individuals, an emerging area of scholarship addresses the effect that the data of one person can have on another person or a group. Perhaps the most obvious example of this is genetic data, which contains information not only about the individual but also about his or her biological relatives and the larger population to whom the individual has hereditary ties.
[2] Ann Cavoukian, Stuart Shapiro and R. Jason Cronk, *Privacy Engineering: Proactively Embedding Privacy, by Design*, Information and Privacy Commissioner, Ontario, Canada, January 2014. Privacy is defined as a "non-functional" requirement because privacy requirements are not required for system operation but may be required for legal compliance, customer trust, risk management, or ethical considerations. Non-functional privacy requirements might lead to additional requirements for the system software or hardware.
[3] European Data Protection Supervisor, *Preliminary Opinion on Privacy By Design*, Opinion 5/2018, May 31, 2018.
[4] World Economic Forum, *Personal Data: The Emergence of a New Asset Class*, January 2011, available at https://www.weforum.org/reports/personal-data-emergence-new-asset-class.

or mobile computing),[5] and in different countries with different legal requirements. IEEE endorses research, process and technology standardization efforts, and education programs, including ethical considerations that support technologists in their work within this complex environment.

- **IEEE supports research efforts to systematize engineering approaches** to designing, implementing, adapting, and evaluating models, methods, techniques, and tools to capture and address privacy issues in the development of socio-technical systems.[6] Development of systematic approaches to addressing privacy would help organizations identify and decrease privacy risks, would enable them to make purposeful decisions about effective implementation of controls in information and communication systems,[7] and would create tools for evaluating and demonstrating compliance with legal frameworks and users' privacy requirements.[8] [9]

- **IEEE supports process and technology standardization efforts in privacy and data governance.** Standards relevant to Privacy Engineering include standardized terminologies, privacy risk assessment methodologies, privacy safeguards and controls,[10] metadata standards,[11] and standardized privacy engineering processes throughout the system development and maintenance lifecycle.[12]

---

[5] *IEEE International Workshop on Privacy Engineering,* 2018, available at http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=69341.

[6] Seda Gürses and José M. Del Álamo, *Privacy Engineering: Shaping an Emerging Field of Research and Practice*, available at https://www.computer.org/csdl/mags/sp/2016/02/msp2016020040.html.

[7] http://csrc.nist.gov/projects/privacy_engineering/index.html.

[8] *IEEE International Workshop on Privacy Engineering,* 2018, available at http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=69341.

[9] Martin Gilje Jaatun, et al, "Towards Strong Accountability for Cloud Service Providers," 2014 IEEE 6th International Conference on Cloud Computing Technology and Science (CloudCom), pp.1001-1006, 15-18 Dec. 2014, available at http://dx.doi.org/10.1109/CloudCom.2014.123.

[10] Privacy safeguards and controls include, but are not limited to, data access, collection limitation, use limitations, etc.

[11] Metadata standards will permit the exercise of individual privacy rights, data portability, data deletion, and compliance with legal and cultural norms.

[12] Examples of privacy standards include ISO/IEC 29100:2011 Privacy Framework, which specifies a common privacy terminology; defines the actors and their roles in processing personally identifiable information (PII); describes privacy safeguarding considerations; and provides references to known privacy principles for information technology. See https://www.iso.org/standard/45123.html. ISO/IEC have also adopted privacy standards for the cloud (ISO/IEC 27018), for specific sectors (health informatics, financial services, biometric identification and others), and have an active effort under way to develop privacy guidelines for consumer goods and services (see ISO/PC 317). The IEEE Standards Association is also engaged in privacy-related standardization efforts and has a number of working groups focused on data protection and governance, including IEEE P7002™, IEEE P7004™, IEEE P7005™, IEEE P7006™, IEEE P7012™, and IEEE P7013™. See IEEE Global Initiative on Intelligent and Autonomous Systems, *Ethically Aligned Design*, v2 for more information about the IEEE P7000™ series: https://ethicsinaction.ieee.org/.

- **IEEE supports education programs** that train technologists in the privacy implications of collection, use and disclosure of personal information, and about business, legal, and policy issues that will influence technical development and deployment of data-rich products and services. Inclusion of courses in ethics, design, data protection law, and public policy in engineering education will help engineers in real-world environments where technical requirements are complemented or constrained by ethical, legal and policy factors. Information about privacy-related standards should be included as part of Privacy Engineering education as well as broader educational programs in engineering, technology, and computing.

- **IEEE supports the engagement of technologists** to improve the understanding of the privacy implications for both individuals and society of technologies, technology related policies, and government regulations affecting personal data.

IEEE endorses the emerging discipline of Privacy Engineering as a systematic approach that supports technologists in their efforts to ensure personal data is only used with full consideration of ethical and legal requirements and cultural norms.

BACKGROUND

Personal data is essential to the development and deployment of new products, applications and services, including the Internet of Things, personalized medicine, remote sensing, and autonomous and intelligent systems (A/IS). However, in order for data-intensive technologies to be fully realized and adopted, they have to be trusted. One aspect of trust is the belief by individuals, businesses, and regulators that personal data will be handled responsibly and will not be misused.

Organizations have been aware for decades of the need to prevent unauthorized access to and use of systems and data. Security Engineering is a discipline focused on identifying and mitigating vulnerabilities that can lead to unauthorized system access and use.[13] With the growth of personal data collection, it has become increasingly clear that products, applications and services that rely on personal information can sometimes function as designed and still violate individual expectations of privacy or legal requirements.[14] Privacy Engineering is the counterpart to Security Engineering,

---

[13] Security is essential for effective implementation of privacy policies and other data policies.
[14] Privacy violations that occur in the absence of security breaches include smartphone apps that collect or disclose data in ways consumers do not anticipate (see, e.g., US Federal Trade Commission settlement with Brightest Flashlight at https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived), data sharing arrangements that violate the law

with the focus on addressing risks associated with planned and authorized functioning of systems that collect, use and disclose personal data.[15]

Privacy Engineers function within multi-disciplinary teams to identify privacy risks and vulnerabilities and to address them through technical and procedural controls.[16] In the past few years companies and government agencies began hiring Privacy Engineers and creating programs that support Privacy Engineering.[17]

The Privacy Engineering discipline is in its early stages of development. There is no agreed-upon definition of the specialization, few standards, and no universally accepted codes of practice. IEEE endorses research, process and technology standardization efforts, and education programs in Privacy Engineering as part of its mission to advance technology for the benefit of humanity.

ABOUT IEEE

IEEE is the world's *largest technical professional organization dedicated to advancing technology for the benefit of humanity. Through its highly cited publications, conferences, technology standards, and professional and educational activities, IEEE is the trusted voice in a wide variety of areas ranging from aerospace systems, computers, and telecommunications to biomedical engineering, electric power, and consumer electronics.*

(see, e.g., UK Information Commissioner's Office findings on data sharing between Google's DeepMind and Royal Free NHS Foundation Trust at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/), and re-identification of data that is supposed to have been anonymized (see, e.g., Jane Henriksen-Bulmer and Sheridan Jeary, "Re-identification attacks—A systematic literature review," International Journal of Information Management, Vol. 36, No. 6, Part B, December 2016, Pages 1184-1192, available at https://www.sciencedirect.com/science/article/pii/S0268401215301262).

[15] National Institute of Standards and Technology, *An Introduction To Privacy Engineering And Risk Management In Federal Systems*, NISTIR 8062, January 2017, available at https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[16] For a variety of technical skills used by Privacy Engineers, see Carnegie Mellon's MSIT-Privacy Engineering brochure at http://privacy.cs.cmu.edu/MSIT-PE-brochure-fall2018.pdf, and IAPP's sample job description for a Privacy Engineer at https://iapp.org/resources/article/privacy-engineer-sample-job-description/.

[17] Carnegie Mellon University offers a one-year degree course Master of Science, Information Technology—Privacy Engineering (http://privacy.cs.cmu.edu). The International Association of Privacy Professionals (IAPP) created a Privacy Engineering section for technologists working on privacy issues (https://iapp.org/connect/communities/sections/privacy-engineering/). The European Data Protection Supervisor created IPEN, Internet Privacy Engineering Network, to bring together developers and data protection experts for privacy-related projects and the creation of new tools to enhance and support privacy (https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en). Australia's Commonwealth Scientific and Industrial Research Organisation (CSIRO) has established a Privacy Engineering project area (https://research.csiro.au/distributed-systems-security/research/technology/privacy-engineering/).