Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304

hp.com

HP Policy Position

Privacy and Data Protection

Current Global State of Privacy and Data Protection

The rapid expansion and pervasiveness of cloud computing, coupled with the explosion of social networking platforms and behavioral-based business models, are attracting renewed policy attention, particularly with respect to privacy and data protection, consumer information stored in the cloud, use of information analytics, and cyber security. HP encourages privacy and data protection regulations that afford a high level of protection, while supporting global business innovation and creative technologies, which need the critical ability to move, and access information across borders.

The U.S. privacy regime largely relies on industry self-regulation, consumer protection through the Federal Trade Commission (FTC), and a mosaic of state laws and industry-specific requirements (e.g., financial services and healthcare). No comprehensive national privacy legislation yet addresses the current technology and business challenges.

The European Union recognizes privacy as a human right, which is primarily governed by the 1995 Directive on Data Protection, complementing directives and national laws. The European Commission is currently updating its broad data protection framework to ensure better harmonization and address adequately the current and future challenges of global data flows and new practices.

APEC is exploring regional harmonization in the Asia-Pacific region, and countries in Latin America are also instituting or updating their privacy and data protection regimes. HP is actively engaged in these efforts with regulators and key stakeholders in the three regions.

HP's Leadership in Privacy and Data Protection

HP as an industry leader in privacy and data protection, is committed to accountability, maintains one of the most robust privacy programs in the world, and actively engages with privacy officials worldwide to strengthen and harmonize privacy frameworks. HP views strong privacy and data protection standards as key to developing and ensuring a secure cloud-based computing environment, enabling the potential of information analytics, and enhancing cyber security while preserving the fundamental right to privacy.

As a consumer-facing company, HP confronts significant reputational risks for any perceived inadequacies in its system for protecting personal data, and considers effective data protection as a key business requirement for current and future ICT offerings. In addition, HP's enterprise and public sector services business manages projects involving personal data for government, health, and financial services clients.

Accordingly, HP maintains one of the most robust privacy and data protection programs in the world, with principles derived from the OECD Guidelines and the EU Data Protection Directive. HP practices are accountability-based, including comprehensive risk assessment, appropriate implementation mechanisms, a state-of-the-art privacy-by-design approach, and an internal audit-approved approach to validation and audit. HP policies are applied globally and map to national and regional laws. In 2001, HP was the first Fortune 50 company to self-certify under the U.S.-EU Safe Harbor Agreement. In addition, HP is one of

the few ICT companies with approved Binding Corporate Rules at the European level — the highest recognition for compliance with the EU Data Protection Directive. Additionally, in 2012, HP's commitment to privacy and data protection resulted in HP being named the Most Trusted Company for Privacy in the Technology and Software Sector — based on a study by the Ponemon Institute.[1]

Privacy and Data Protection: Impact of New Technologies

Cloud

The cloud refers to the ability to access and rapidly scale up or down computing power, data storage, and processing resources on demand from a remote data center, while paying only for the resources used.[2] Clouds can be private, community, public, or hybrids, depending on ownership and use. The cloud has the potential to rapidly increase efficiencies, partnerships, and productivity, while dramatically reducing costs by dynamically assigning resources and optimizing data centers. An organization is still responsible for protecting the privacy of data stored in the cloud. HP seeks to leverage its established leadership in privacy issues in shaping privacy regulations, including those pertaining to cloud, that ensure the highest level of protection for individual privacy rights while supporting business objectives and innovation.

Big Data and Information Analytics

"Big data" is revolutionizing the way we apply algorithms and analysis to very large, diverse data sets. Big data is already being used to identify trends and unlock key discoveries in areas such as healthcare, financial fraud, cyber security, weather prediction, scientific research, and education.

Big data differs from traditional analytics in that rather than verifying and validating assumptions based on statistical samples, it uses all the data to discover correlations between diverse data sets. Sophisticated tools and methods allow scientists to mix data sets together, including "unstructured data," such as video, voice, and social networking.

Data protection governance is key to protecting fundamental rights and assuring individual trust. That means applying innovative data protection tools in new ways to meet the objectives that come from data protection principles. One such approach that is garnering attention is to split big data into two phases. The first phase, "discovery," is essentially research, and requires security and procedural protections to assure the data used in discovery is not personally impactful. De-identification of data used in big data projects is one such strategy. The second phase, "application," may well be personally impactful and requires a privacy-by-design approach.

HP is taking a leadership role in evolving data governance to assure society reaps the benefits of big data while still protecting individual privacy. This work is taking place both in multi-stakeholder groups and at HP Labs.

---

[1] *2012 Most Trusted Companies for Privacy*, Ponemon Institute LLC, January 28, 2013, *available at* http://www.ponemon.org/local/upload/file/2012%20MTC%20Report%20FINAL.pdf.

[2] *The NIST Definition of Cloud Computing*, Peter Mell & Timothy Grance, National Institutes of Technology, U.S. Department of Commerce, Special Publication 800-145, September 2011, *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf; *Unlocking the Benefits of Cloud Computing for Emerging Economies – A Policy Overview*, Peter Cowhey & Michael Kleeman, University of California San Diego, released November 2012, *available at* http://irps.ucsd.edu/assets/001/503998.pdf, at 1, 6.

HP believes accountability is critical for big data governance and is applicable beyond private sector activities as governments are potentially major users of big data processes. Therefore, to assure public trust and allow the public sector to take full benefits of these new practices, HP believes that accountability practices should be applied to the public sector as well as the private sector.

Cyber Security

The increasing volume of cyber security threats and risks faced by consumers, enterprises, and governments alike has ushered in a new era in which policymakers are increasingly seeking to address cyber security through legislation and regulation. HP supports positive efforts by governments to enhance defenses against the many and evolving cyber threats, without mandating use of "one-size-fits-all" technologies or approaches. Use of effective data protection and privacy practices by government and corporations will enhance cyber security by protecting personal information from potential threats.

HP believes that well-defined data breach notification requirements have the potential to increase trust and protection. Nevertheless, to avoid excessive reporting of minor breaches, minimum criteria should be established for triggering the obligations to notify, even in the case of notification to the supervisory authorities.

HP's Policy Recommendations

HP's vision of privacy and data protection is based on four core principles:

1. *Fundamental Right:* Privacy is critical to fundamental rights and requires appropriate protection.

2. *Accountability:* Companies should make responsible, ethical, and disciplined decisions about personal data and its use through the data's lifecycle. Furthermore, companies should be accountable as good stewards of the data provided to them. For these reasons, HP strongly supports clearly articulated and well-defined accountability principles in privacy regulation. HP believes that binding self-regulatory mechanisms with third-party verification either by regulators or accountability agents, such as Binding Corporate Rules (BCRs) and the APEC Cross-Border Privacy Rules (CBPRs), are excellent means both to ensure compliance and demonstrate that a company has a comprehensive and mature data protection program in place.

3. *Global Harmonization and Interoperability:* Around the world, HP strongly supports international policy convergence and efforts that will ensure the interoperability of privacy and data protection frameworks. In order to achieve international interoperability, HP has been deeply involved in working with governments all over the world, including efforts to create the Madrid Resolution on International Privacy Standards; review the OECD Privacy Guidelines; implement the European Binding Corporate Rules (BCRs) framework, and develop implementation mechanisms for the APEC Cross-Border Privacy Rules. HP is also actively engaged with regulatory authorities at the country level, where we are often invited to share experiences and opinions in developing these countries' secondary privacy regulations.

4. *Fluid, Flexible Tools to Address an Ever-Evolving Global Marketplace:* Given the complexity and the dynamic nature of global commerce, current and future challenges cannot be addressed with pre-defined, highly prescriptive solutions that are necessarily based on the understandings we have today. Fluid, flexible, principles-based solutions are needed to ensure compliant and effective privacy and data protection. To ensure their efficacy, such solutions must be based on commitments to over-arching concepts with a comprehensive approach, focusing on results and expectations and not only on the means employed to achieve them. Regulators are considering some of these concepts, such as the legal right to process, privacy-by-design, and others.

United States

- HP urges policymakers to establish baseline federal legislation that clearly articulates expectations for all organizations. Such legislation would strengthen the chain of accountability, allowing consistent compliance versus the divergent regulations currently in force. Importantly, it would also address the very real need for consumer protection, while giving industry the flexibility to innovate in a responsible manner.

European Union

- From the beginning, HP has voluntarily aligned its policies and practices with the principles of the EU Data Protection Directive on a global scale. Currently, HP seeks to help address the practical barriers to implement the proposed EU Data Protection Regulation.

- Specifically, HP would like to see a greater role of accountability in the regulation, BCRs for controllers and processors, a more balanced approach to traditional consent and control in the case of new technologies, and well-defined data breach notification requirements with minimum thresholds and realistic response timeframe. HP welcomes the inclusion of privacy-by-design practices in which companies build privacy protections into products and technologies.

- HP has actively participated in the development of BCRs for data processors. Companies participating in the implementation of such a mechanism will extend protection of data even into jurisdictions that have not been deemed adequate by the EU. This will allow for greater protection while permitting services companies that process data for others to move work through their supply chain.

Asia Pacific

- HP has been a permanent participant in the APEC Data Privacy Sub-group and has decided to become one of the first companies to be certified under APEC's CBPR mechanism once accountability agents have been approved. APEC and the EU are collaborating to achieve interoperability between BCRs and CBPRs, which could become the foundation of interoperable privacy regimes that will allow companies to move data lawfully around the world on the basis of accountable practices.

- HP encourages Asia-Pacific economies to become part of CBPRs. HP considers that the work being done in APEC on interoperability through third party verified binding co-regulation will enhance privacy protection and benefit both companies and data subjects.

Latin America

- Latin America has been a source of innovation in privacy regulation. HP has worked closely with governments in the region to develop their privacy regimes. Nonetheless, some work still needs to be done. Countries in Latin America have an opportunity to create modern privacy regimes that incorporate new concepts and enhanced protection. HP also believes that countries in the region need to become part of interoperability mechanisms such as CBPR's. Latin America should undertake a more regional approach on privacy, focused on interacting with BCR and CBPR measures in Europe and Asia Pacific.