



Testimony of Scott Taylor
Chief Privacy Officer, Hewlett-Packard Company
Before the Committee on Commerce, Science and Transportation
of the U.S. Senate

June 29, 2011

Chairman Rockefeller, Ranking Member Hutchison and Members of the Committee, my name is Scott Taylor and I am the Chief Privacy Officer at Hewlett-Packard Company. Thank you for inviting me to testify today on privacy. HP commends the Committee for its forward-looking approaches to balancing consumer privacy interests with the business realities of a global, Internet-based economy.

We are living in a time when our reliance on technology is increasing every day. There is a continued blurring between our business and personal lives. Consumers are more dependent on mobile devices, and they have a growing expectation that companies will be accountable stewards that respect and protect the information we collect, use and maintain.

Today's technologies provide tremendous benefits to consumers and businesses and are critical to economic growth and prosperity. Yet these same innovations create new challenges related to privacy.

Privacy is a Core HP Value

HP's core values of trust, respect and integrity provide the foundation for our commitment to privacy. HP firmly believes that our ability to succeed in the marketplace depends upon earning and keeping our customers' trust. HP has a rigorous global privacy program and is at the forefront of industry efforts to create new frameworks and strengthen privacy protections. HP takes active steps to implement organizational accountability for privacy throughout our company. We believe companies need to do more and be willing to demonstrate their capacity to uphold the obligations and commitments they make.

Accountability Framework

HP's approach to privacy is built on a model of accountability. We seek to create a chain of accountability for the information we handle, ensuring data privacy and security are advanced at every stage of the process. HP teams work together to oversee and manage our privacy efforts and collaborate with external partners to advance privacy protection worldwide.

HP's privacy accountability model is a decision-making framework that helps business units make informed choices about the risks associated with collecting and handling data. Our accountability approach demonstrates HP's commitment to privacy and goes well beyond legal compliance. Various factors are taken into consideration including first and foremost ethics as well as contractual agreements, regulations, international provisions and corporate culture. Our model builds on that foundation by considering decisions in light of our company values, customer expectations and potential risks to ensure we are fully accountable for our actions.

To that end, we have built a robust internal privacy program that focuses on integrated governance, risk and opportunity identification. Combined with strong policy commitments and senior management support, our program encourages transparency, ensures policies are instituted and validates program effectiveness. The diagram below demonstrates HP's privacy governance model:



HP monitors compliance with its privacy policies using internal assessments, customer and employee feedback, and internal audits. Our privacy team works closely with the HP Ethics and Compliance Office and internal audit function to align with their approaches to compliance. All suppliers and third-party vendors that handle HP customer and employee personal data are contractually bound to comply with applicable portions of our privacy policies and detailed supplier security standards.

Privacy and Data Protection Board

HP's Privacy and Data Protection Board (PDPB) provides company-wide oversight for privacy and personal data protection. The PDPB comprises executives from Privacy, Legal, Information Technology, Security, Internal Audit, Procurement, Internet, HP Labs, Human Resources and the Global Government Affairs functions, as well as from each business unit and region.

At quarterly meetings, the PDPB members discuss strategy and high-level priorities, assess programs, launch projects and resolve any issues identified through our ongoing monitoring programs that have been escalated to the PDPB. The PDPB regularly invites external experts to discuss privacy trends and developments. The PDPB conducts an annual risk assessment and the members work throughout the year on teams that handle specific privacy issues and mitigation projects. For example, as a result of the PDPB's work, all company laptops are required to have full-disk encryption to mitigate the risk of data theft or loss.

The PDPB enables HP to manage data protection risks comprehensively in a seamless and integrated way. Its shared risk assessment and decision-making model sets a standard for governing information management more broadly.

Privacy by Design

HP designs privacy and data protection into new products and services, guided by comprehensive, company-wide privacy standards for product and service development. This builds consumer trust and provides a competitive advantage for HP. The concept of considering privacy from inception is referred to as “Privacy by Design” and is one of the fundamental elements in the legislation of Senators Kerry and McCain that HP supports.

For corporate customers, HP’s Secure Advantage portfolio offers hardware, software and services that help protect data throughout its lifecycle, whether it is stored on a desktop, laptop computer, a printer or in a data center. Privacy features incorporated into the portfolio include:

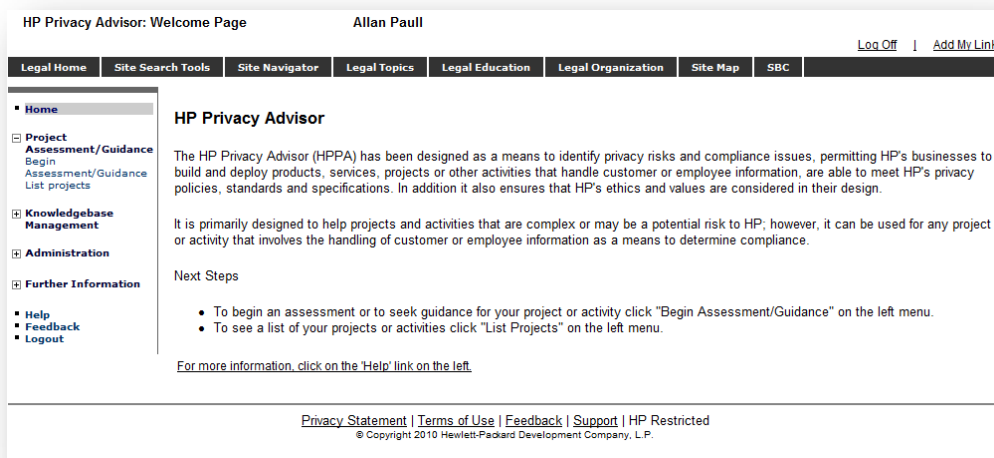
- Software that asks the user whether they want to be notified when updates are available, rather than sending notices and installing updates automatically.
- Full-disk encryption that helps protect the data on each drive, even if the disks are lost or stolen, with minimal impact on performance.
- Automated encryption devices to increase protection.

HP scientists who support our privacy team continue to work on several collaborative research projects on privacy. For example, they lead Ensuring Consent and Revocation (EnCoRe), a partnership of six organizations with the goal of making it safe and easy for people to give and withdraw consent for their data to be used. HP scientists and engineers are working with eleven other companies on another project called Privacy and Identity Management for Community Services (PICOS) to create confidence in the safety of sharing data in online communities. Project members are identifying privacy, trust and identity management issues and plan to design and build mobile communication tools to address these issues.

Privacy Advisor Tool

Beyond our privacy team, at the core of our implementation strategy is the HP Privacy Advisor tool that integrates our privacy philosophy and commitments into an end-to-end program to better educate and guide our employees about privacy requirements, risks and considerations. This interactive tool helps to ensure that as we develop new products and services, privacy considerations are integrated from the first stages of development. Coupled with employee education and mandatory training, this tool helps to hold every employee accountable for privacy and data protection.

HP's privacy team partnered with our R&D labs to develop and deploy a Privacy by Design program to ensure that our more than 300,000 employees understand privacy implications as they conceive and develop products and programs that will collect or use personal data. Below is a screen shot that shows HP's Privacy Advisor tool:



Importantly, the tool is not just about compliance. It integrates ethics and values-based considerations to ensure we align to company codes of conduct and consumer expectations. If we think about most product designers or marketing managers, they are thinking about the next

innovation and their first priority isn't necessarily privacy. Whether employees are designing a new product or launching an email marketing campaign, they need to understand how to put policies, obligations and values into effect. And they need to do so as they design new products and prior to deployment.

Not all innovative ideas become reality, so we need to break down product or program development into simple stages. In the design and development stages, HP's privacy team provides proactive guidance so privacy considerations can inform early planning. This has traditionally been difficult for companies and can result in a program being delayed or cancelled later based on privacy concerns.

Early guidance related to privacy becomes tremendously valuable to the organization because it ensures privacy pitfalls can be avoided. In the deployment, maintenance and end-of-life stages, our privacy team does more than just guide. They provide assessment mechanisms to ensure compliance with laws, company obligations, policies and values. We have learned that this assessment needs to be as contextual as possible. For example, the way we need to assess privacy compliance in a global email campaign is very different than in a new PC or web-enabled printer that seeks to deliver a customized user experience.

The HP Privacy Advisor tool is available to every employee from our internal Internet portal. Employees log in using a digital badge that authenticates their credentials and identifies them and their organization. That information is also used to assign the appropriate privacy team member for follow up.

Here is a screen shot of the employee login page:

The screenshot shows the 'Project Information' tab of the HP Privacy Advisor. The form is titled 'Project/Campaign' and contains several sections:

- Project/Campaign:** Includes fields for Project/Campaign Name (Test Project), Project/Campaign Region (Asia Pacific), Lead Business Group (WW Legal), and Lead Organization (Legal E and C).
- Additional Information:** Includes a text field for 'This is a test'.
- Project Description:** Includes a text field for 'This is a test'.
- Project Lead:** Includes a text field for 'Allan Paul' and a checkbox for 'Same as below'.
- Project Lead Email:** Includes a text field for 'allan.paul@hp.com'.
- Contact:** Includes fields for Contact Name (Allan Paul), Contact Title (APJ Region Privacy Officer), Organization (Legal E and C), Business Unit (Legal), Business Group (WW Legal), Region (Worldwide), Contact Phone (+81 411 232 249), and Contact Email (allan.paul@hp.com).

There are several notes on the right side of the form:

- NOTE:** On this screen general information about the nature of your project is collected. It should give a privacy expert a high level idea who is doing the project and what it is about.
- The field marked with the symbol * are mandatory and you need to fill them before continuing.
- The 'Project Lead' is the employee responsible for or managing the project/activity. If the project lead is the same as the contact person for the project then please check the "Same as below" checkbox.
- The field marked with "*" are mandatory and need to be completed.
- If you need to provide access to other team members, you can share this project or the report from the List Projects page after it is created. By Sharing a Project you can have one project lead and multiple contributors to the same Project.
- The resulting questionnaire is dynamically built from the project or activity profile determined by the "Project Profile" section and from the answers to other questions in other sections. So the length of the assessment or the amount of questions that you will have to answer depends on the nature and complexity of the project. A simple project may not take long to assess however a complex project will take longer.

At the bottom of the form, there is a 'Continue' button and a note: 'It will take 30 minutes or more to enter a project/activity into this tool depending on the complexity of the project/activity.'

The tool starts by asking simple, basic questions about the proposed project. As each question is answered, additional dynamically-generated questions are posed based on the collective intelligence and risk factors derived from how prior questions were answered.

Below is a look at sample project profile questions:

The screenshot shows the 'Project Profile' tab of the HP Privacy Advisor. The form contains a question:

NOTE: This section presents questions that the tool uses to build up a basic profile of your project and to tailor follow-up questions in upcoming sections accordingly.

Does your project or activity (product, application, service, campaign, etc.) handle customer or employee information?

Yes Not Sure No

At the bottom of the form, there are three buttons: 'Back', 'Save and Continue', and 'Save and Exit'.

The HP Privacy Advisor tool is an intelligent privacy impact assessment mechanism that is geared to the employee user and scales from simple to complex programs. One of the greatest benefits is educating employees in the context of their program or work tasks. Through the process employees learn about privacy issues and can modify their approach to ensure compliance. The following two graphics show additional questions based on the sample project:

Project Information | **Project Profile** | Data sources/Data Flows | Transparency | Project Specifics | Harm Indicators

NOTE: This section presents questions that the tool uses to build up a basic profile of your project and to tailor follow-up questions in upcoming sections accordingly.

Does your project or activity (product, application, service, campaign, etc.) handle customer or employee information?

Yes No Not Sure [Help with question](#)

Would you like the tool to provide privacy guidance or provide a privacy assessment of your project or activity? Please select either Guidance or Assessment mode.

Privacy Guidance Privacy Assessment [Help with question](#)

Which information categories does your project or activity handle? (check all that apply)

Customer information Other Employee information

[Back](#) [Save and Continue](#) [Save and Exit](#)

Project Information | Project Profile | Data sources/Data Flows | Transparency | Project Specifics | **Harm Indicators**

NOTE: This section is used to determine and identify any aspects of your project that indicate the possibility for privacy related harm. The previous answers suggest that your project or activity may require legal and HP Privacy review. Have you consulted and reviewed your project or activity with your legal counsel or with the HP Privacy?

Yes No Planned Not Sure [Help with question](#)

Has the project or activity already begun handling the individual's information prior to privacy approval of the project?

Yes No Not Sure [Help with question](#)

Is what you are doing something that might surprise the individual, or something they may not expect, or outside typical industry practices or norms?

Yes No Planned Not Sure [Help with question](#)

Are proper access controls to information clearly defined, implemented and verified that they will work as defined?

Yes No Planned Not Sure [Help with question](#)

Does your project or activity, or your vendor, implement controls to prevent the loss or corruption of data that could cause harm?

Yes No Planned Not Sure [Help with question](#)

How long do you plan to keep the information?

Only for this purpose Longer than 12 months 6 months Not Sure 12 months [Help with question](#)

Is your implementation or program something that may be a new use of information?

Yes No Planned Not Sure [Help with question](#)

Does your project or activity have processes to honored opt-outs to marketing contact?

Yes No Planned Not Sure [Help with question](#)

Do you have sound business reasons to collect the information you are asking for, when considering the purpose/s of what you are actually attempting to achieve?











Yes No Planned Not Sure [Help with question](#)

[Back](#) [Finish](#) [Save and Exit](#)

The assessment results are documented and reviewed by the privacy team. Consultation is provided as necessary. If any issues exist, approval from the privacy team is required prior to deployment. After a product or program launches, triggers exist to ensure deployment was consistent with expectations and that end-of-life actions are taken when appropriate. The image below shows a report of the sample assessment results:

Detailed information per compliance/risk indicator

This section provides detailed information on your project or activities assessment. It displays this information by Compliance/risk indicator providing a visual indicator of status with detailed reasons behind each assessment.

-  **A. Transborder data flows** [Return to graph](#)
Related to transfer of information across national borders.
-  **B. Compliance** [Return to graph](#)
Related to compliance with either HP or external standards, policies, laws, and other requirements.
-  **C. Other** [Return to graph](#)
Related to risk indicators not specified.
The project or activity has been found to have unanswered questions, questions where the answer "Not sure" or "Do not know" has been provided or your answers indicate there may be a moderate privacy risk. A moderate privacy risk may indicate that there are areas of your project or activity where improvements can be implemented to lessen the risk.
 -  The target market tends to be privacy sensitive. [Why this result?](#)
 -  You have indicated that you are conducting email marketing in New Zealand. New Zealand has implemented Anti-Spam laws that HP will need to comply with. [Why this result?](#)
-  **D. Business controls** [Return to graph](#)
Related to "out-of-the-box" business processes and sharing data with third parties (logical HP, vendors, outside third parties).
The project or activity has been found to be in compliance or have a low privacy risk in this section.
 -  You have indicated that the contact preferences of the intended recipients of the e-mail marketing message is "Yes". This is in accordance with HP Policy. [Why this result?](#)
-  **E. Sensitivity** [Return to graph](#)
Related to a sensitive market (i.e., elderly, children, etc.) and/or sensitive data (data related to an individual granted some measure of special treatment, i.e., health or medical conditions, finances, sexual behavior).
-  **F. Transparency** [Return to graph](#)
Related to transparency in the areas of notice/user messaging and choice/consent.
-  **G. Data control** [Return to graph](#)
Related to control of the data lifecycle (i.e., collection, usage, quality, and/or retention).

By using technology, we are better positioned to scale our privacy team's knowledge and guide our 300,000 employees to think about privacy in the right context and at the right time. Nothing is perfect, but we think it goes a long way to minimizing unanticipated effects, and balances our ability to innovate and ensure responsible practices when using data.

An Integrated Framework For Privacy Will Benefit Consumers

Since 2006, HP has worked closely with the U.S. Congress, the Federal Trade Commission and the U.S. Department of Commerce to establish a new strategy for federal legislation. We have long advocated for comprehensive federal privacy legislation which we believe will support business growth, promote innovation and ensure consumer trust in the use of technology. The complexity of existing state laws and statutes can make it difficult for businesses to comply with the law. We firmly believe it is time for the U.S. to establish a comprehensive, flexible and legal framework for protecting consumer privacy. Recent research from University of California, Berkeley and the Pew Research Center tells us that consumers are becoming more concerned, and increasingly want to know that their privacy is protected. We believe consumers are expecting federal legislation, companies need it and the economy will be better for it. Federal legislation would also help us compete in the global marketplace since a baseline privacy law in the U.S. allows the opportunity for international interoperability.

In addition to our work in the U.S., HP is actively engaged with Data Protection Commissioners in Europe and the Binding Corporate Rules (BCR) of our privacy program have been approved by the European Union. BCR approval is considered the highest level of certification for organizational privacy accountability. In Asia, HP helped create and shape the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules system. We are actively engaged in forward-looking frameworks in Latin America as well.

In preparation for this hearing, the Committee asked that we examine three privacy bills: (1) S.799 – The Commercial Privacy Bill of Rights Act of 2011; (2) S. 913 – Do-Not-Track Online Act of 2011; and (3) S.1207 – Data Security Breach Legislation. We support the concepts espoused in all three of the bills and look forward to further collaboration with the Senate Commerce, Science and Transportation Committee, government regulators and industry to craft privacy and security laws that enable robust and rapid innovation, appropriate consumer protection, greater consistency and predictability. We look forward to continuing our engagement and furthering the efforts to increase effectiveness of the U.S. legal framework for the protection of privacy and data security. Below are our brief thoughts on each of the bills.

S.799 – The Commercial Privacy Bill of Rights Act of 2011

HP supports this innovative legislative effort by Senators Kerry and McCain. As stated earlier in the testimony, “Privacy by Design” is one of the fundamental elements in the bill and is a practice HP fully embraces. We look forward to working with Congress to advance this legislation.

Earlier this year, HP joined Microsoft, eBay and Intel in supporting the Commercial Privacy Bill of Rights Act of 2011 introduced by Senator John Kerry (D-MA) and Senator John McCain (R-AZ). Our four companies released a joint statement in support of the bill:

We are pleased that Senator Kerry and Senator McCain, both long-time advocates for strong consumer privacy protections, have introduced the Commercial Privacy Bill of Rights Act of 2011. We support the bill and look forward to working with Congress as it moves forward.

We have long advocated for comprehensive federal privacy legislation, which we believe will support business growth, promote innovation and ensure consumer trust in the use of technology. The complexity of existing privacy regulations makes it difficult for many businesses to comply with the law.

We support the bill's overall framework, which is built upon the Fair Information Practices principles. We appreciate that this legislation is technology neutral and allows for flexibility to adapt to changes in technology. The bill also strikes the appropriate balance by providing businesses with the opportunity to enter into a robust self-regulatory program.

We look forward to continuing our engagement to improve the effectiveness of the U.S. legal framework for the protection of privacy.

S. 913 – Do-Not-Track Online Act of 2011

HP interacts with consumers and businesses in many ways online, including the sales and support of our products and services. We believe that the adoption of new innovation depends on companies acting in an accountable and responsible manner to anticipate and advance consumer needs. No one is served – not corporations, not governments and certainly not consumers – by a lack of customer confidence in the security and privacy of personal information. At HP, we believe consumer trust comes from transparency and providing meaningful choice to consumers. Accordingly, we support the concepts in Senator Rockefeller's do-not-track legislation.

With the acquisition of Palm, HP owns and operates WebOS (an operating system used in HP products). HP sells our WebOS devices configured to ensure we do not track location-based data without active user consent. When a user opts to enable location services, the data is used only for diagnostic purposes and is not shared or sold externally. Other products and services, such as our PCs, Internet-enabled printers and other mobile devices, provide similar levels of consumer transparency, choice and strong privacy protections.

We would welcome the opportunity to collaborate with Senator Rockefeller to ensure consumers are given appropriate choices for tracking in a manner that recognizes existing industry standards and technology limitations. We encourage industry to develop new standards to facilitate more meaningful choices across a consumer's online experiences.

S.1207 – Data Security Breach Legislation

Both as a consumer products company and as a service provider to other companies, HP collects and maintains personally identifiable information. Over the last 10 years, almost every state in the U.S. has adopted a data security breach law. The patchwork of state laws and statutes in existence today confuses consumers about their protections in any given context, and forces companies to contend with differing and often conflicting regulations. In some cases the laws require over-notification which does nothing to increase privacy protection. This is why we strongly support initiatives like Senator Pryor's data security legislation, which would set a single, national, preemptive standard. Such a law would create consistency and predictability for businesses and better protection for consumers.

We support the concepts and principles of the draft bill and look forward to providing input on the guidance documents. We hope to ensure that any notice required would be meaningful and useful in preventing identity theft or other related harms that may result from a data breach. In particular, notification must be prompt to enable the impacted individuals and companies to take appropriate action to protect themselves. That said, the notification timeframe must take into account the complexity and nature of the data and the breach. Moreover, the communications vehicles must be effective in reaching the intended audience and should include new media platforms when appropriate (e.g., chat rooms, social media, email, etc.).

Closing Statement

We continue to urge policymakers to examine ways to establish baseline federal legislation that will clearly articulate expectations for all organizations. As more and more services are delivered through multiple parties, such as applications on mobile devices, a consistent baseline standard will strengthen the chain of accountability and unify the divergent regulations currently in existence. We believe this responds to the very real needs of anxious consumers, and gives industry the flexibility to innovate in a responsible manner.

Stated simply, HP recognizes that consumer trust is a precious commodity that must be protected through good stewardship and robust privacy programs. Federal legislation can establish the baseline for organizational accountability and improved consumer protection. It's a win for both consumers and the industry as a whole.