BEFORE THE

DEPARTMENT OF COMMERCE

OFFICE OF THE SECRETARY

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

INTERNATIONAL TRADE ADMINISTRATION

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Request for Comments

INFORMATION PRIVACY AND INNOVATION

IN THE INTERNET ECONOMY

DOCKET# 101214614-0614-01

COMMENTS OF

Intuit Inc.

January 28, 2011

Barbara Lawler
Chief Privacy Officer, Intuit

2700 Coast Avenue
Mountain View, CA 94043

Intuit thanks the Department of Commerce for the opportunity to comment on the proposed dynamic framework for commercial data privacy and innovation, and commends the Department's Internet Policy Task Force for their extensive work to evaluate the current business climate with regard to consumer privacy and business innovation and its thoughtful work in discussing the framework.

About Intuit

Intuit was founded in Silicon Valley more than 25 years ago, and is dedicated to solving important problems by using technology to simplify financial management for consumers and

small business. Our mission on behalf of consumers and small businesses is to provide products, services and tools that improve our customers' financial lives so profoundly that they cannot imagine going back to the old way. In addition to the commercial enterprise, Intuit's mission as a corporate citizen is also carried through more than a decade of philanthropy that enables eligible lower income, disadvantaged and underserved individuals and small businesses to benefit from our tools and resources for free.

Today, we are the nation's leading provider of tax, financial management and online banking solutions for consumers, small and mid-sized businesses, accountants and financial institutions.

Our familiar brands, TurboTax (www.turbotax.com), Quicken (www.quicken.com), Mint (www.mint.com), and Quickbooks (www.quickbooks.com) are designed to help our customers -- individual taxpayers, consumers, and small businesses -- to improve their financial lives. This means: we help them make or save money, be more productive, and be in compliance. For example, Intuit makes it easy for any small business owner to get customers, get paid, pay employees, track sales and expenses, and do financial and tax planning. We do this by organizing, displaying, summing, and using our customer's information as triggers for alerts to serve their needs and requirements.

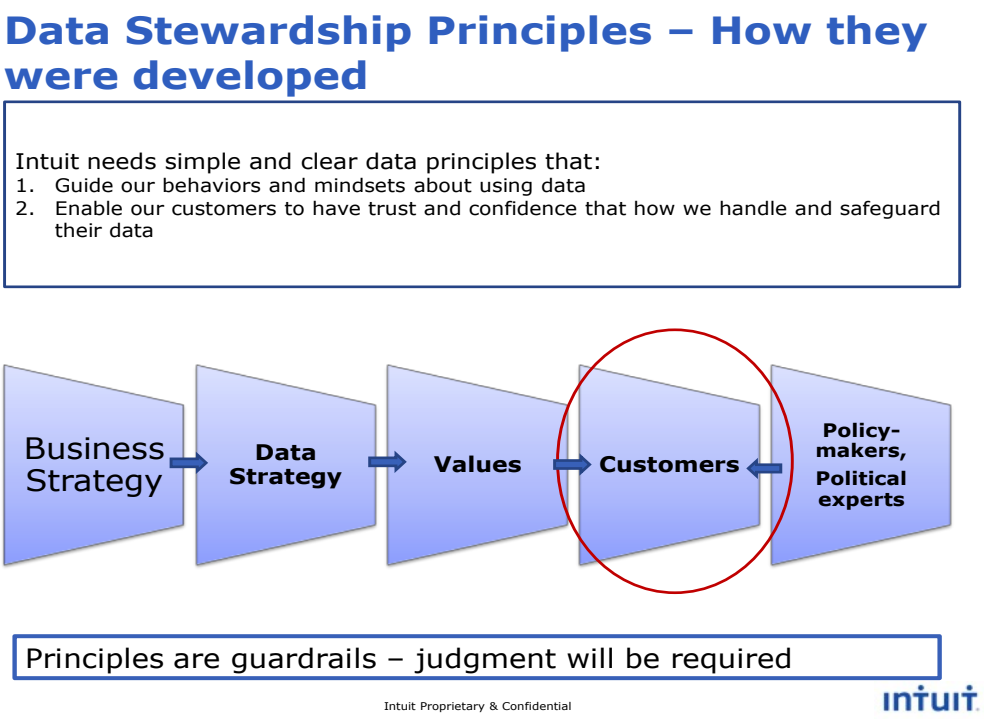
Intuit also helps consumers manage their health and medical expenses. Among other offerings, Intuit cooperates with several health plans to provide *Quicken Health*^{sm} *Expense Tracker*; a service that gathers medical expense information in one place, enabling the consumer to find and correct errors, to make medical expense payments easily, and to transfer relevant information smoothly to their income tax returns.

Intuit is pleased to see that the Department of Commerce recognizes the importance of balancing the respect for the consumer control of information with the need for innovation. Intuit's data- or information-driven business is one that is consumer driven. We believes our policies and practices which emphasize customer control already illustrate that a company can act as a steward of customer information and still be a successful, innovative company.

The Intuit Philosophy and Strategic Approach to Data

Intuit's customers entrust us with their most sensitive data, including: their federal and state income tax return information; their individual purchase transactions, including health information; their business accounts: employee payroll, accounts receivable, vendor lists, inventory and other business data. We are widely recognized and respected for our strong privacy and security practices. Maintaining our customers' trust is critical to maintaining our business. Recognizing that importance has led our experienced privacy team to undertake a formal examination of how we inform our customers about how and what information we collect, process, use and then protect, so that the customer may understand what we do, know what to expect from us, and actively choose to participate.

Our formal examination included reviewing our company value system (notably our first business value which underpins everything we do: Integrity without Compromise), our privacy policies, and our data use practices. This review helped us articulate what we stand for. We then formed an aligned and informed philosophy that we term "Data Stewardship Principles" that guide our use of information in our products and in business operations. The principles have undergone thorough review within Intuit, including extensive research in our customer community, and with external thought leaders.

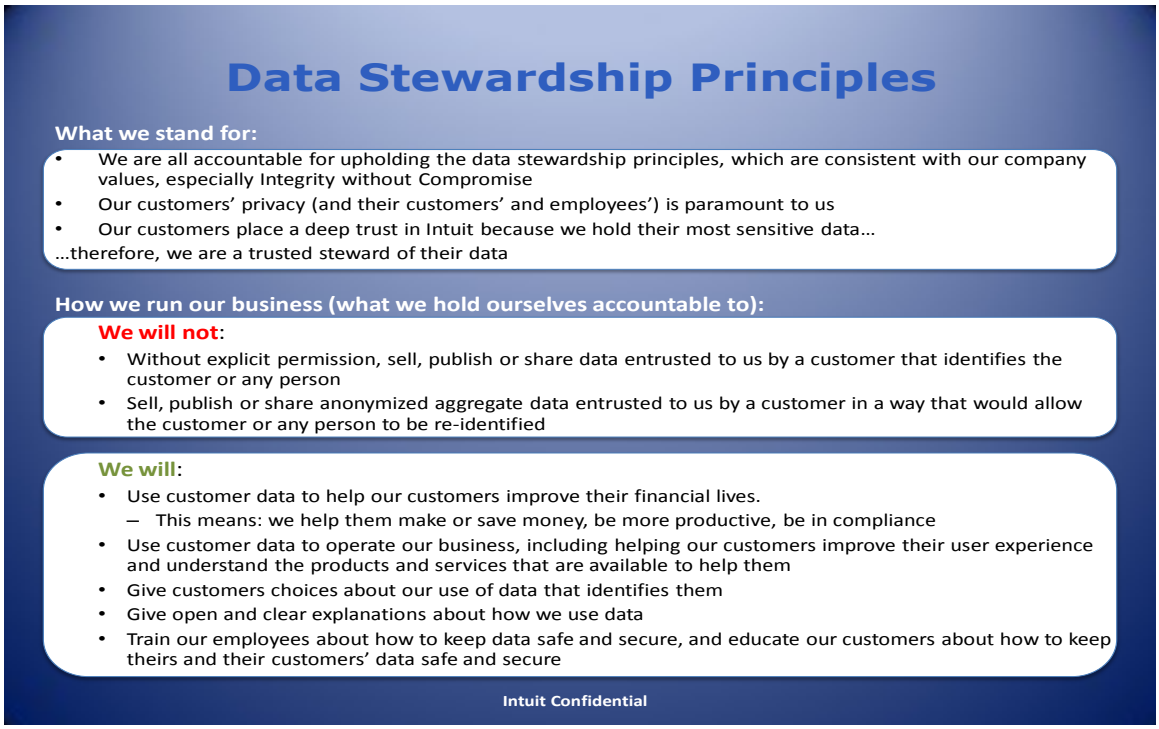


"Accountability" is the foundational principle for Data Stewardship, both as a concept and Intuit's internalization of that concept. Intuit has participated with the Center for Information Policy Leadership[1] as part of the Accountability Project[2] which built on ideas in the OECD Guidelines, the EU Privacy Directive, and the work in forming the APEC Privacy Framework, as well as US and state law. Accountability is a central tenet in Intuit's treatment of our customer's information: we will be accountable for the information entrusted to us. We will provide explanations of why we ask for information that may be sensitive; we will give choice in whether information is disclosed to another organization; we will hold our service providers to the same standards we hold ourselves. Of course, we will use customer information in normal business operations: to maintain customer lists for marketing; to bill our service subscribers; to provide shipping information to our fulfillment vendors; to complete payment processing; and to determine how our products and services are being used so that we may improve them. By design, our Data Stewardship Principles align closely with globally recognized fair information

[1] http://www.hunton.com/Resources/Sites/general.aspx?id=45 Reviewed January 21, 2011

[2] http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf Reveiwed January 21, 2011

practices, although there is not a one-to-one correlation with the DHS FIPPs presented by the Department of Commerce. They are more closely matched with FIPPs for online privacy developed in the late 1990s. As we have learned, we believe the Principles identified below are the ones that carry the most weight and meaning to consumers, based on an extensive research process we will describe below.



The Proposed Dynamic Privacy Framework Alignment with Intuit Philosophy and Strategic Approach

- **Promoting entrepreneurship, innovation and economic development**

Intuit believes that any U.S. consumer privacy framework should empower and protect consumers, enable innovation in the 21st century, and enhance global competitiveness. Our products and services are inherently both data-driven and customer-driven. Customers use our products and services to manage their personal lives and businesses, 24/7. Trust is woven into the user experience –m our customers know what to expect from us. They look to Intuit to improve and simplify their lives in ways so profound that they won't go back to their old way of doing things. As Intuit looks to the future (where our customers are going; where the marketplace and technology is going) we see an ever-increasing pace of change and expectations from current and future customers. Both new offerings and enhancements to existing offerings will employ more and more sophisticated, rich, real-time interactive use of data. To retain consumer trust in that context, Intuit's vision is that privacy and security are central to the concept of customer "delight", and therefore serves as a competitive advantage. For innovation to succeed, creative re-use of data, under a Data Stewardship regime, is a must. The essence of

Data Stewardship cannot rely on just one element of our principles, it must be comprised of all of them combined: customer driven innovation coupled with responsible and novel data innovation. Moreover, as global competitiveness evolves beyond the bricks-and-mortar economies of the past, and international trade takes on an electronic character in the economy of the future, sound business practices and wise public policy are critical components of innovation, invention, and full, fair and open competition. Attached is a link to our Intuit 2020 Report for your reference: http://http-download.intuit.com/http.intuit/CMO/intuit/futureofsmallbusiness/intuit_2020_report.pdf

- **Protecting informed choice and individual privacy in order to promote user trust**
- **Transparency, Individual Participation and Accountability**
    - **Transparency and Individual Participation**

Our 27-year history of customer-driven innovation is part of the DNA of how we run our business every day. As we developed and refined our Data Stewardship Principles, it was our normal course of action that we would take our customers along with us on the journey to define our value principles around the use of data in a way that reflects the needs, concerns and values of our customers. We took draft Data Stewardship Principles directly to our customers and asked them for their feedback, on both the concepts and words, on both intent and practical, real-world customer experience and expectations. We conducted 2 rounds of quantitative, statistically valid surveys that cut across multiple customer bases and product lines to get feedback and learn if Data Stewardship and Privacy mattered to them, which principles and how much. We conducted 2 rounds of qualitative customer focus group sessions to dive deeper into the subtleties of transparency, choice, data use cases and security.

Staying true to customer-driven innovation, we iterated and refined the Data Stewardship Principles over the course of the customer research process. Here is what we learned in summary.

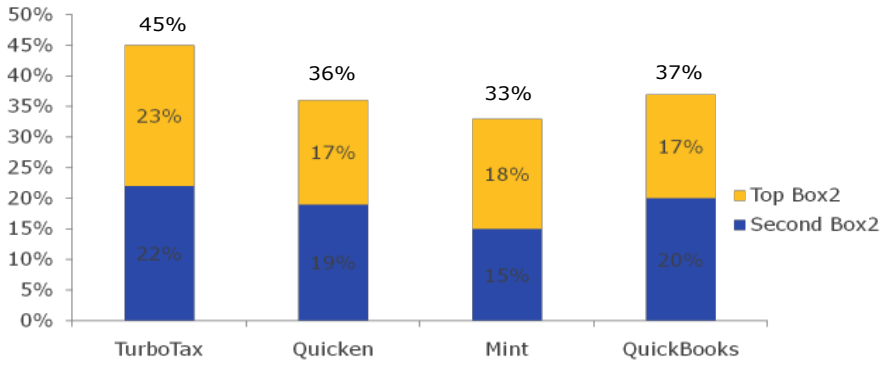
- After several rounds of input and iteration, the Principles have been extremely well received:
    - Customers may not read privacy policies but care deeply about how their data is used;
    - Consumers are smarter than some give them credit for…..they are aware of a wide range of data uses, to benefit them directly and for necessary internal business operations.
    - While a majority of our customers already have a positive impression of Intuit, the Data Stewardship Principles further built trust.
    - Across all research studies, the principle around not selling or sharing data is the most important.
    - The more transparent (meaning open, simple and clear) the company is, customer trust increases and their need for detailed and frequent or repetitive choice mechanisms appears to decrease.

  Training employees to uphold these principles is also important to customers and adds an incremental level of trust that we will deliver against our promises.

Customer Trust and Confidence Baseline

Current Overall Level of Trust…Before Exposure to Principles (baseline)

Overall, our customers have a high level of trust in Intuit.
Trust improves the longer a customer is with Intuit.



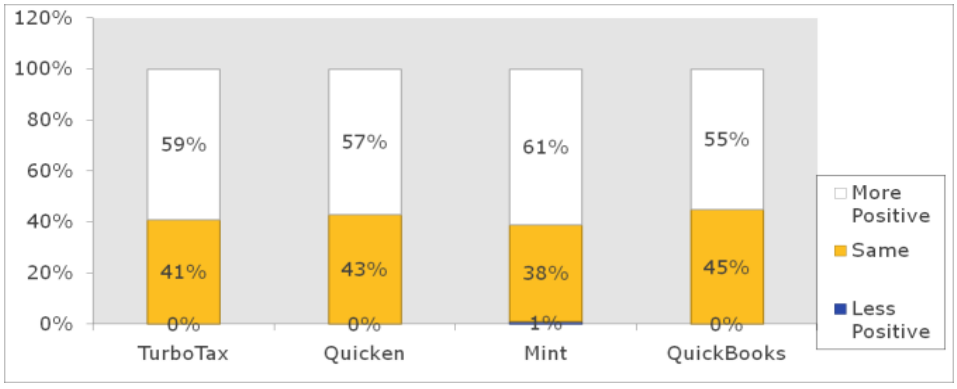
Rating on a scale of 1-10. Top Box=10, Second Box = 9.

intuit

Customer Trust and Confidence increases dramatically after reviewing Data Stewardship Principles

Impression of Intuit…After Exposure to Data Stewardship Principles

The majority feel more positive after reading the principles.



intuit

- Here are a few illustrative verbatim statements from our customers that show what Intuit's Data Stewardship Principles mean to them:

- *"This is what makes customers trust them. I like that privacy is paramount & do believe they're committed to this."*
- *Customer focused, protecting my data and interests, holding themselves accountable."*
- *"I like that these principles are VERY SPECIFIC. There is no doubt, or any way to not understand EXACTLY how Intuit intends to treat my information. I like that."*
- *"Because of these principles, I will continue to use their products."*
- *"A little safer in an unsafe world."*

When customers participate directly in the shaping of Data Stewardship Principles, it brings to life the FIPPs concepts of Transparency and Individual Participation in profound ways. Intuit believes policymakers and regulators can learn from our experience and our customers' feedback. Specifically, we have learned that a principle-based approach to privacy that is not prescriptive is substantive and meaningful to consumers, and will provide more flexibility in adapting to a wide range of industries and data uses, innovation and invention.

Intuit will continue to research the impact of Data Stewardship Principles on customer behavior, focused on transparency and choice, using experience design and A/B testing techniques, and can make a summary of those results available, when the research is complete, if the Department is interested.

Risk and Compliance Assessments, Accountability and Validation

Intuit, along with many in industry, uses a blend of risk and compliance assessment to validate that day-to-day business practices and technologies apply Data Stewardship Principles, and Privacy and Security Policies and Standards. Enterprise Risk Management, Audit, Compliance, Security and Privacy functions may provide that capability. Third Party resources may be brought in to assist assessment and compliance verification.

It should be noted that Accountability (see Accountability Project reference p.4) is more than risk and compliance assessments and validation or audits. Accountability is the sum of all promises (e.g. Data Stewardship Principles) an organization makes and the many mechanisms in place to make those promises real. It must include training and awareness building, substantive executive sponsorship, governance bodies, performance metrics and reporting, business model analysis, along with the aforementioned risk and compliance validation.

A wide range of criteria, external and internal, may be incorporated into these validation processes. External criteria may derive from 3rd party accountability agents such as TRUSTe or the Better Business Bureau, from technology or industry standards such as Payment Card Industry requirements or SSAE16, from government-industry agreements such as the U.S.-E.U. Safe Harbor Agreement or the APEC Privacy Principles Pathfinder Cross Border Privacy Rules, and of course from laws, regulations and enforcement actions.

One of the many mechanisms by which these assessments are conducted is through Privacy Impact Assessments (PIAs) and Security Evaluations.

Privacy Impact Assessments

Intuit uses various types of reviews to ascertain that a new offering will provide appropriate protections for its users and meet our expectations and promises. Some reviews are relatively simple interviews to make sure that an enhancement to a current offering doesn't change its current protections. Others are extensive because the offering will process sensitive data in an area new to Intuit or to our customers. The assessments themselves may cause changes in the offering so that it meets our standards or it may require additional explanation in a privacy statement and other transparency mechanisms so that the customer may understand how data is being gathered, processed and used. The assessments themselves are not made public but help Intuit to understand its practice and to be able to describe it clearly for others.

Generally, a PIA covers what data will be collected (from whom, from where and by what method), where it will be stored, what external and internal systems will provide or receive the data, who has access to it and how long the data will be retained. These questions enable the privacy and security team, working together, to determine what risks must be mitigated in order to provide appropriate protections. We'll know if an application is Internet-based, or on a SmartPhone, whether it needs location information, if the data is to be transferred to another entity (like IRS), and whether its treatment is governed by specific laws and regulations.

Intuit believes the detailed elements of a PIA should be set by the entity collecting and processing information. That entity should develop its PIAs with knowledge of the type of business, type of information, kinds of customers, appropriate codes of conduct, and applicable laws and regulations. Commerce might consider developing a PIA framework that could inform organizations in their development of more detailed PIAs.

Intuit encourages the Commerce Department to proceed carefully around the idea of publicizing Privacy Impact Assessments to enhance transparency. As we've described, PIAs are internally-focused tools and their structure and content vary widely. In the context of enhancing consumer understanding and transparency, PIAs, as they exist and are used today, could be just as mystifying to consumers as so many published privacy policies and statements across industries are as a practical matter today. And because published privacy practices (whether by policy, statement, just-in-time notice, or PIA) are promises enforceable under FTC Section 5, we suspect many companies would be reluctant to publish a distinctly separate set of information (from published privacy polices and statements) about data handling and privacy practices via PIAs. This topic merits further, deeper discussion between the Department and industry.

- **Giving existing and emerging Internet companies more consistency, uniformity, and predictability in the privacy protections expected by consumers and required by law**

Intuit urges that the Department recognize that different applications of data can and should have different requirements and different safeguards. Tax return information, such as that collected in the use of the TurboTax product, is already governed by a strict, specialized set of requirements under IRS Regulation 7216. Some uses of data are essential to delivering services and applications over the Internet, whether they be online services such as Quicken, Mint.com, QuickBooks Online, Intuit Online Payroll or Intuit Go Payment. Collecting information for use in routing a request on the Internet should have different standards for transparency, acceptable uses, protection, and retention than the information collected to describe a patient's visit to a

physician, payment processing or an electronic transfer of funds to a bank account. Each deserves protection but the shields for the identity of persons in medical studies, for example, need to be stronger and last longer because the information must be retained longer to serve its purpose. It is the use of the information as well as its characteristics that should inform our treatment of it. Context is crucial.

- **Increasing efficiencies for online companies by bringing industry players together with consumers to fashion cohesive and consistent practices; and**

Enforceable Codes of Conduct

Intuit is intrigued by the idea of multiple, sector-specific, enforceable codes of conduct. Using the general baseline principles and ideas garnered from subject matter experts, reasonable codes could be developed which would encourage innovation and yet protect the consumer. We strongly welcome the Department's proposal to convene multi-stakeholder forums to develop codes of conduct (or a set of practices/standards for small business to follow), and look forward to participating in such an effort. Intuit's experience in multiple sectors has taught us that providers and consumers of information in the health sector, for example, have different requirements and expectations for protection than do those in financial services. Although these sectors have laws and regulations defining some of the protections, these sectoral differences are not well understood by Data Protection Authorities outside the United States. Using a law delineating fundamental privacy principles, the enforceable codes could account for the differences and still meet the need for a single regime of privacy protections. Subject matter experts could help inform the development of appropriately balanced codes. A spectrum of codes are in existence today…from recent work in online advertising, to longer-standing frameworks like the U.S.-E.U. Safe Harbor Agreement (and related compliance programs in place from TRUSTe and the DMA), E.U. Binding Corporate Rules, the emerging APEC Cross Border Privacy Rules and Privacy Seal Programs. Each of these codes has an element of enforcement, typically by the Federal Trade Commission today, a role the FTC should retain.

Each code would need an entity to "own" and administer it. Industry, Trade Associations or best practices organizations like TRUSTe, the Better Business Bureau, the Direct Marketing Association, Interactive Advertising Bureau, the Mobile Marketing Association, and Small Business Administration offer a range of potential ways to administer the codes of conduct. These types of organizations are experienced in raising awareness and in registering and tracking members. This would address any concerns about adding to the burden of government activity. Line of business industry associations, such as those that exist for Dentists, Florists, or Building Contractors may provide effective mechanisms to reach and teach small and medium businesses unaware of privacy and security expectations of their end customers.

We envision a tiered approach where the statute would enumerate the basic protection principles, with pre-emption of state laws to eliminate the differences and conflicts in triggers, reporting requirements, and breach definitions, and then leave the sectoral rules to the enforceable codes of conduct or their current regulatory regime. Clearly, some sort of transition plan would be necessary to give time for the development of the codes. Enforcement of the codes should be the

province of the current appropriate regulators and/or the administrator of the code. Should that fail, then the Federal Trade Commission would provide the appropriate enforcement action.

Intuit, then, supports the idea of codes of conduct that are enforceable. Multi-stakeholder participation (civil society, business, regulators, consumers themselves) in the development of the codes will allow the important differences amongst data uses to be recognized and accounted for. An advantage that codes of conduct have over law is that they may be amended much more easily. We would recommend that the code development process include provision for a regular, periodic cycle for review and amendment to address unforeseen changes in the environment.

Intuit is open to the idea of baseline, principle-based privacy legislation that could work in tandem with codes of conduct. It must be a principle-based approach that is not prescriptive and enables flexibility to work within a wide range of data use contexts and existing sector privacy laws. Intuit is in the unique position of already working under multiple sector-specific privacy laws, to which we can speak about the strengths and weaknesses of each. A principle-based approach could fill the gaps, crevices that exist between the differing sector approaches, while at the same time blending with them. A principle-based approach is more likely to be received and effectively adapted by all businesses, including small businesses or spectrum of businesses not actively engaged in the privacy landscape. A principle-based approach is more likely to be understood by the public it seeks to protect. And a principle-based approach is more likely to achieve consensus over time in the international context, which will be essential to global competitiveness in the emerging digital economy.

Such an approach could set forth a minimum set of requirements for business, and provide a fundamental, core level of consistency for businesses and consumers. Codes of conduct, based on context, industry/sector, technology platform or other data use drivers would build on top of a privacy baseline.

Privacy Policy Office

Intuit believes that the Department of Commerce and its proposed privacy office is an appropriate agency to convene stakeholders in developing the multi-party enforceable codes of conduct. As a representative of the Executive branch, DoC can lead the development of American policy in a way that the independent Federal Trade Commission cannot. The Federal Trade Commission, as an enforcement agency and as the agency representing the consumer, is, of course, a critical stakeholder. Commerce, however, can and should develop and execute policy on behalf of the Executive Branch and its mission to make American business more innovative at home and more competitive abroad.

We particularly look forward to DoC leadership in working toward Global Privacy Interoperability, and related international policy principles pertaining to data stewardship, and in convening the appropriate stakeholders to develop the Enforceable Codes of Conduct.

- **Reducing barriers to trade and commerce that stem from disparate privacy standards and requirements in different nations**

Competition is a hallmark of American enterprise. However, we also have concepts of fair play and "level playing fields". One rocky playing field experienced by American companies with business in more than one international jurisdiction is preserving the free flow of information, while respecting the various country law and regulations with somewhat conflicting goals. The United States and the DoC clearly need to participate and champion the concept of safe and secure information flow in all relevant international discussions. It is as important to the future of international trade and commerce in the emerging digital economy of the 21st century as any rules and regulations that governed and refereed trade and commerce in the bricks-and-mortar economies of the 19th and 20th centuries.

While so many laws and regulations are based on essentially the same principles, multi-state and multi-nation companies are challenged by the differences among them. Some regulations in breach notification, for example, require notification of some state agencies; others don't. The notification triggers and thresholds are different. And the definitions of important terms vary across the landscape. In a domestic context, we support a uniform federal breach notification law. Aligning practices across states would provide benefits for consumers who purchase from merchants in other states. It would also lessen the complexity for merchants, a consistent goal in improving the economy. In an international context, baseline principles that meet the E.U. and APEC principles would improve multi-national commerce, allowing the freer-flow of transactions across borders and thus improving our ability to export. Intuit agrees that the U.S. government should continue to work toward increased cooperation among privacy enforcement authorities around the world and develop a framework for mutual recognition of other countries' frameworks. Intuit agrees that the U.S. should also continue to support the APEC Privacy Principles Pathfinder Project, because it is the best framework to achieve data privacy interoperability in the 21st century.

Intuit agrees with the need for a Federal standard and framework for data security breaches. We also favor state pre-emption and further alignment at the federal level (e.g. between the FTC and HHS for health information).

Electronic Surveillance and Commercial Information Privacy

Intuit supports updating ECPA, as long as it it done in a way that protects individuals from unwarranted government intrusion in the online world. We urge the government to keep in mind that ECPA goes hand in hand with CALEA (a statute that ensures technology is capable of being tapped by law enforcement and surveillance organizations). There should not be different rules for communications content and non-content data. We believe reform in this space is critical to enable global interoperability and to the overall growth of the digital economy.

Intuit appreciates the opportunity to provide comments on the Dynamic Policy Framework for Data Privacy and Innovation. We eagerly await the opportunity to help move the strategy forward.