COMMENTS OF HONEYWELL, INC.
ON FTC's FRAMEWORK FOR PROTECTING CONSUMER'S PRIVACY

Honeywell, Inc. ("Honeywell") respectfully submits these comments on the FTC's preliminary report on a framework for protecting consumer privacy in an era of rapid change. Specifically, Honeywell comments on policy issues surrounding the need to balance enhanced consumer privacy protections while encouraging innovation. As a leader in several consumer-oriented markets including energy management systems (e.g. thermostats, SmartGrid solutions), home security systems and bar-code scanning solutions, Honeywell is uniquely aware of the implementation challenges associated with striking such a balance.

I. COMMUNICATIONS

All correspondence, communications, pleadings, and other documents relating to this proceeding should be served upon the following persons:

Amy Chiang
Vice President, Government Relations

Honeywell International
101, Constitution Ave. NW, #500W
Washington DC 20001

Telephone: (202) 662 2638
Fax: 202-662-2675
Email: amy.chiang@honeywell.com

Dr. Sanjay Parthasarathy
Technology Strategy Leader

Honeywell International
101, Constitution Ave. NW, #500W
Washington DC 20001

Telephone: (612) 356 3512
Fax: 202-662-2675
Email:
sanjay.parthasarathy@honeywell.com

II. BACKGROUND AND EXECUTIVE SUMMARY

Honeywell is a global provider of software and hardware solutions and services that run industries, secure buildings and protect critical infrastructure. Secure information access, data integrity, and privacy are the underlying tenets in Honeywell's development methodologies. We strongly support the FTC's tenets for ensuring privacy while encouraging innovation:

- ***Privacy by Design*** – firms need to build in privacy during product development, and re-visit policies routinely.
- ***Simplified Choice*** – customers should be empowered in making decisions regarding the sharing of their data.
- ***Improved Transparency*** – firms need to provide consumers with clear and simple notifications and access to their data when requested.

Honeywell believes that to adequately ensure data privacy, security and integrity, the FTC's framework should:

- Minimize the amount and sensitivity of data sent outside of the consumers' realm.
- Share consumer data only when the consumer explicitly opts-in to a sharing program.
- Protect the data in transit, as well as the data at rest.
- Apply strict privacy policies that limit how third parties process the data and with whom they may share it.

III. COMMENTS

A. SCOPE OF THE FTC FRAMEWORK

Honeywell supports the FTC's decision to apply the framework to all commercial entities that collect or use consumer data. Additionally, Honeywell recommends that commercial entities that collect, maintain, share, or otherwise use consumer data should be required to take the following steps:

- Localize high-fidelity data collection to devices in close user proximity;
- Link only less granular information (e.g. energy consumption by minute stored locally, but broader trends by hour sent to the "cloud");
- Periodically (e.g., bi-annually) re-evaluate privacy policies;
- Provide individuals with the option to opt-in or opt-out of data sharing agreements; and
- Provide the ability to push privacy-enhancing software updates to user devices.

Additionally, Honeywell supports oversight of the aggregation of non-sensitive consumer data, such as data that is used solely to test, measure, validate or verify the efficacy of regulated programs. This oversight is necessary because of the potential for aggregators to gain access to private consumer data. For example, demand aggregators in the SmartGrid industry need reliable estimates of sheddable load during peak electricity events. To obtain such data, aggregators query utility companies to gain access to coarse data on consumer loads and the probability of customers responding favorably to a shed event. Although utility companies typically mask consumer data and organize query responses by zip code, time of day, or type of consumer, it is possible for aggregators to make

multiple queries[1] that allow for the recovery of private data[2] that cannot be extracted by a single query type. FTC oversight of these aggregation methods will mitigate the risk that private consumer data will be obtained.

With respect to energy consumption, current initiatives in "Connected Homes" and "SmartGrid" utilize consumers' energy consumption patterns to deliver energy savings. Energy consumption data is essential for optimizing energy use and cost; however, we believe that detailed energy consumption data that describes a customer's living or business pattern should be considered private. Thermostats and energy management systems designed for placement in consumer homes should help consumers optimize their comfort and minimize their costs while protecting their privacy. One such product is the Home Energy Manager which empowers consumers to determine access criteria for any third-party firm and since the device is physically located inside a consumer's home, it is controlled by the consumer at all times. This technology minimizes transmission and storage of sensitive consumer data at a central database thereby minimizing the probability and severity of data compromise and the subsequent loss of privacy.

B. PRIVACY BY DESIGN

The FTC framework should require companies to build privacy considerations into their product development and product lifecycle while ensuring

[1] An Evaluation of the Current State of Genomic Data Privacy Protection Technology and a Roadmap for the Future, http://www.truststc.org/wise/articles2009/articleM1.pdf

[2] Predicting Social Security numbers from public data, Alessandro Acquisti1 and Ralph Gross, Carnegie Mellon University, Pittsburgh, PA 15213 http://www.pnas.org/content/106/27/10975.full.pdf

that consumers have reasonable access to their own data. Honeywell also recommends that privacy settings and preferences be required to be "backwards compatible" – i.e., they should work on existing products and devices in consumer's homes so that these products and devices do not have to be replaced by the consumer. In addition, there are several initiatives in cyber-security that can ensure data access is restricted to only those authorized. Examples include:

Authentication: Honeywell encourages the FTC to adopt a policy that supports the development and deployment of strong individual and machine authentication mechanisms. The mechanisms should be used to strongly authenticate email, access to web pages, Internet based transactions, remote control functions (e.g. smart grid enabled energy management), electronic medical records and sensitive interactions between citizens and the Government.

Federated and cooperative authentication: Honeywell encourages the FTC to adopt additional safeguards to protect consumer data that, if compromised, could have a potential impact on energy infrastructure or markets. Today, when an individual wants to view numerous websites on the Internet, he or she must obtain multiple authentications to gain access to each website. Certain technologies, however, allow an individual to authenticate once and then obtain a secure token that identifies the various systems and data to which the individual is seeking access. Those systems and data will allow access based on the secure token contents that meet specific gating functions into the data. Similar technology allows for delegation of access rights so that a user can provide a third party temporary rights to access the user's data. Honeywell recommends that the FTC

require companies that store consumer data in the cloud to encrypt the data or incorporate authentication or authorization protocols to prevent the compromise of consumer data.

Data Retention: Regarding data retention, Honeywell recommends that the FTC require data to be retained only as long as it is needed. Companies should be required to obtain consumer consent to archive or access data beyond its stated "shelf-life." Companies also should be required to participate in internal audits that monitor compliance with industry standards.

Liability Legislation: Honeywell supports the FTC's development of policies addressing the liability associated with use, acceptance and the potential compromise of strong authentication. The Government has protected its citizens via laws providing information privacy and establishing liability for compromise of privacy. We believe that liability legislation will further drive privacy considerations in product development.

C. SIMPLIFIED CHOICE

Honeywell believes that empowered consumers are the engine for economic growth and new business models. However, to empower consumers, choices must be clear, concise and complete. The benefits of technology should be explained, and the resulting data access requirements must be stated before the consumer signs on for the service. We believe that consumer data should only be shared when consumers expressly opt in to such programs. We encourage an opt-in model for all privacy-related data, including applications like the SmartGrid.

To ensure consumer privacy and opt-in choices, Honeywell recommends requiring companies to obtain user consent at the point of sale and to follow up during each consumer interaction thereafter. For instance, consent also should be verified when configuring any related devices, software or services; and whenever new services or software updates are offered or purchased. An icon that appears consistently on the purchased devise may help to alert the consumer that their consent is needed and to inform them of their privacy options. A similar icon for secure transactions is currently being used on browsers when consumers shop on "safe sites."

The FTC's framework should promote open market participation, which, in turn, will encourage innovation and investment in new technologies. Competition will ensure availability of better and cheaper products. We have gained experience from the telecommunications market, where innovation and competition have made cell phones and cell phone services very affordable even to low-income consumers.

Finally, Honeywell believes that Deep Packet Inspection plays a vital role in security but may violate consumer privacy requirements when used to track user behavior when executing transactions. Deep Packet Inspection should ensure that the data source and destination are valid, malware is detected and the data integrity is maintained when in transit. However, gathering consumer-specific information or behavioral patterns within the data stream under the auspices of Deep Packet Inspection is not appropriate.

D. IMPROVED TRANSPARENCY

Honeywell believes that engaging consumers is necessary to improve transparency and will require a balance of education, ongoing incentives and simple choices during initial participation. For example, Honeywell helps utilities manage their peak demand by curtailing customer's loads. Our experience has shown that migration from opt-in model to an opt-out model in such 'demand response' programs can change results dramatically. Even in an opt-in situation, participation results can vary from slight below 10% or soar to greater than 30% when there is a tailored education program.

IV. CONCLUSION

In conclusion, Honeywell supports the proposed framework proposed by the FTC and we encourage the FTC's collaboration with the administration, industry, academia and regulatory bodies to protect consumer privacy interests. To ensure data privacy, security and integrity, Honeywell recommends that the FTC framework promote the following goals:

- Minimize the amount and sensitivity of data sent outside the consumers' realm.
- Share consumer data only when the consumer explicitly opts in to a sharing program.
- Protect the data in transit, as well as the data at rest.
- Apply strict privacy policies which limit how third parties may process the data and who they may share it with.