June 2, 2016

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230
Attn: IOT RFC 2016

Submitted electronically to iotrfc2016@ntia.doc.gov

Nest Labs, Inc. ("Nest") appreciates the interest of the Department of Commerce ("Department") in the technologies comprising the Internet of Things ("IoT") and welcomes the opportunity to provide comments on the benefits and challenges associated with these technologies and the government's role in fostering their advancement. Nest believes there is much that the public sector in general, and the Department in particular, can do to help the IoT economy flourish, in particular promoting a regulatory climate that encourages innovation at this early stage of IoT development.

I. Introduction

A. About Nest

Founded in 2010, Nest is dedicated to reinventing everyday home products like thermostats and smoke alarms to create a thoughtful home that takes care of the people inside it, while addressing societal challenges such as energy consumption and life safety. Nest products are sold in the United States, Canada, the United Kingdom, Ireland, France, Belgium, and the Netherlands.

Nest manufactures the Nest Learning Thermostat, a smart thermostat equipped with multiple sensors (for example, temperature, humidity, and motion sensors), Wi-Fi capability, and processors running software to help customers stay comfortable and consume less energy. The Nest Learning Thermostat combines inputs such as manual adjustments provided on the device or through the Nest mobile app, occupancy patterns, and advanced algorithms to learn a household's temperature preferences, adjust heating or cooling when the house is empty and automatically lowering air-conditioning runtime when humidity conditions permit.

Nest also manufactures a connected home security cameras, Nest Cam, which provides 24/7 live streaming to customers' phones to help them monitor their homes, find out if something is wrong, watch their pets, or simply to know if a package has arrived. By using audio and video algorithms, Nest Cam can detect motion and sounds that are out of the ordinary and alert customers of unusual activity. Nest Cam can even turn on automatically when a home's occupants leave the dwelling by using location data from the user's phone (if the user decides to enable this feature) or through an integration with a Nest Learning Thermostat.

Likewise, Nest manufactures Nest Protect, a connected smoke and carbon monoxide alarm that uses advanced sensor and communications technology and sensing algorithms to alert users to smoke and carbon monoxide emergencies, speak verbal warnings, and provide a record of recent safety events. Like Nest's other products, Nest Protect can send alerts to users' phones and can be managed remotely through the use of a mobile app, for example to silence a false alarm.

Nest products work together in thoughtful ways. For example, owners of Nest Protect can have Nest Cam automatically start recording when Nest Protect sounds an emergency smoke alarm (to help them see what happened). They can also have Nest Learning Thermostat turn off the furnace in a carbon monoxide emergency to eliminate the most likely source of carbon monoxide intrusion into the home.

Finally, Nest runs the Works with Nest developer program where developers can obtain access to the Nest cloud API to build integrations between Nest products and services and third-party products and services that result in new experiences for customers of both products. For example, Nest Protect works with smart light bulbs via the Works with Nest program to flash lights red and turn them on (to aid in egress) when Nest Protect sounds a smoke alarm.[1] The Nest Learning Thermostat works with washers and dryers to have the appliances go into economy or wrinkle-free modes when the Nest Learning Thermostat senses the house is empty and goes into away mode. The Works with Nest program has more than 18,000 developers, including leading product manufacturers and energy, insurance, and security companies.

B. Fostering the Advancement of IoT

Internet-connected "smart" devices equipped with sensors and actuators like those made by Nest are finding widespread application in a variety of environments, including

[1] Nest Labs, https://nest.com/works-with-nest/ (last visited June 2, 2016).

wearables, vehicles, factories, cities, agriculture, medicine, and, of course, the home. The particular benefits and public policy issues raised by IoT will vary depending on their context. Nest's comments are directed to the area where it is most active — connected products in the home, or "residential IoT."

A generation ago, we stood at the dawn of a new and transformative set of technologies — the Internet and the World Wide Web. We are now at the early stages of another transformative application of computing. The Internet, when combined with sensors installed in a wide range of environments and the power to derive insights from the data they collect, offers enormous and still largely unrealized benefits. By one account, IoT is expected to add $14.2 trillion to the global economy, adding a full percentage point to GDP in twenty major markets, over the next fifteen years alone.[2] According to that report, if those economies increase IoT investment by 50 percent, their GDP could increase by 1.5 percent.[3] By 2030, IoT is expected to add $6.1 trillion in cumulative GDP to the U.S. economy alone, and could add up to $7.1 trillion with additional investment — raising U.S. GDP by 2.3 percentage points higher than trend projections.[4] Fostering a vibrant, flourishing IoT calls for the same balanced, pro-innovation approach to regulation that the government applied to the Internet in the 1990s. That approach, which largely reserved the exercise of government authority to address demonstrable, concrete harms in specific circumstances, enabled previously unimaginable opportunities in communications, media, e-commerce, and countless other areas.

This is not to say that companies involved in the development and deployment of IoT technologies are or should be unconstrained. To the contrary, agencies like the Federal Trade Commission ("FTC") have well-established consumer protection authorities, which they are already employing to police IoT products and services just as they do other technologies. Governments should be cautious of blue sky efforts to catalogue theoretical future harms and forestall them through mandatory regulation or other government intervention, lest they miss the mark and dampen innovation. NTIA and other government actors should follow the highly-successful model of regulation that helped pave the way for the emergence of today's thriving information economy.

---

[2] ACCENTURE, WINNING WITH THE INDUSTRIAL INTERNET OF THINGS HOW TO ACCELERATE THE JOURNEY TO PRODUCTIVITY AND GROWTH 2 (2015), *available at* https://www.accenture.com/us-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Digital_1/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.pdf.

[3] *Id.* at 3.

[4] *Id.*

II. The Tremendous Benefits and Opportunities of Residential IoT

Residential IoT presents enormous opportunities for consumers. Nest's products, for instance, help consumers save money by using energy more efficiently, resulting in lower greenhouse gas emissions, and, through partnerships with energy companies, can help to balance peaks in electricity demand and reduce consumption through voluntary seasonal adjustments to the customer's heating and cooling schedule.[5] These products can also help consumers remain safe and secure in their homes and open new frontiers of engagement between consumers and their homes. Through partnerships with insurance companies, Nest is able to foster adoption of residential IoT by helping consumers save money on insurance premiums and receive rebates in connection with the purchase and use of Nest Protect.[6] While we are excited about these capabilities, even benefits like these only scratch the surface of the potential consumer benefits from residential IoT.

While attention has often focused on IoT as premium products aimed at tech savvy, "early adopter" audiences, connected technologies in the home also hold significant potential for a broad range of people, including the disabled, seniors, and economically-disadvantaged communities. For instance:

- ***Increasing Accessibility for the Disabled***. Because connected devices can respond to varied inputs (for example, button press, in-app controls, or voice commands) and may be designed to interconnect with equipment manufactured specifically to provide accessibility, residential IoT can help individuals with disabilities control their environments and live more independently. For example, a wheelchair-bound person may be able to control a connected device from a nearby smartphone, and a person who is hearing impaired may receive supplemental alerts through connected flashing light bulbs or mobile device notifications.

- ***Helping Seniors Age in Place.*** As our population ages, smart home devices will in the future be able to help seniors retain autonomy in their homes, improving their quality of life. For example, connected devices can remind seniors to take their medication and refill their prescriptions. Smart home devices could also help adult children, wherever they are located, to confirm that their aging parents are staying active, eating properly, taking their medicines, and

[5] Nest Labs, https://nest.com/energy-partners/ (last visited June 2, 2016).
[6] Nest Labs, https://nest.com/insurance-partners/ (last visited June 2, 2016).

remaining safe and secure in their homes, all of which can help seniors continue to live independently with greater assurance and assistance than conventional technologies provide.

- ***Helping Low Income Communities Save Money.*** Nest is similarly optimistic about the benefits that energy-saving devices like smart thermostats can provide to low income communities by saving on their monthly utility bills. Third-party studies have shown that the Nest Learning Thermostat can help US customers save an average of 10-12 percent on heating and 15 percent on cooling bills,[7] and Nest is exploring how these benefits may manifest in low-income communities for whom reductions in monthly heating and cooling costs would be especially consequential.[8]

In addition, residential IoT can provide aggregated, anonymized data that can be helpful for research in the public interest. For example, aggregated, anonymized data sets based on carbon monoxide events in the home can deepen researchers' understanding of the nature and prevalence of CO buildup, whereas in the past, such research has generally relied on self-reporting or after the fact forensic investigation. Insights such as these can help inform decision-makers on how best to address public safety challenges and improve life safety for consumers and first responders.[9]

III. The Role of Government in Promoting the Development of IoT

Nest appreciates the constructive, pro-technology approach NTIA has outlined in its Request for Comment and expects that the private sector will stand ready to serve as a resource and partner in the Department's future efforts to help secure for all Americans the benefits of advanced connected technologies. Nest proposes a variety of considerations to help guide the federal government's thinking as it considers IoT issues moving forward.

- *First*, Nest recommends that the Department keep in mind (and encourage other governmental actors to keep in mind) the tremendous benefits -- present and

---

[7] NEST LABS, ENERGY SAVINGS FROM THE NEST LEARNING THERMOSTAT: ENERGY BILL ANALYSIS RESULTS (Feb. 2015), *available at* https://nest.com/downloads/press/documents/energy-savings-white-paper.pdf.

[8] *See, e.g.*, White House Office of Press Secretary, *FACT SHEET: President Obama Announces New Actions to Bring Renewable Energy and Energy Efficiency to Households across the Country* (Aug. 24, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/08/24/fact-sheet-president-obama-announces-new-actions-bring-renewable-energy.

[9] NEST LABS, NEST PROTECT CARBON MONOXIDE FIELD STUDY: RESULTS FROM NOVEMBER 2013 TO MAY 2014 (June 2014), *available at* https://nest.com/downloads/press/documents/co-white-paper.pdf.

future -- of connected technologies. These including (but are by no means limited to) those described above with respect to residential IoT. It is entirely appropriate for regulators to assess the challenges that innovation presents, and Nest applauds the Department's interest in issues such as shifting notions of privacy, consumer control, and data security. At the same time, it is crucial in these important discussions that the underlying benefits of innovation and new technologies remain central in policymakers' minds, as they are in consumers' daily lives.

- *Second*, the Department should continue to promote public-private collaboration. Projects like NIST's Smart Fire Fighting Initiative,[10] and its work on cyber-physical systems, are already exploring, clarifying, and demonstrating new use cases for connected technologies.[11] They are also helping to stimulate discussion among relevant public and private actors and should be encouraged and expanded. By partnering with industry, government actors can better understand the potential benefits of connected technologies in myriad environments. Likewise, Nest encourages government agencies at both the state and federal level to consider connected products, and the services they are capable of providing (such as energy savings and demand response services), as user-friendly, increasingly widespread options for meeting existing policy objectives.[12]

- *Third*, the Department should promote, through its own efforts and by its interactions with other government actors, a pro-innovation climate. Just as policymakers in the 1990s accorded the Internet room to develop into the extraordinary engine of dynamism and economic growth it has become, so policymakers today should adopt a similar approach for IoT. Accordingly, policymakers should avoid regulations based on speculation about the direction,

---

[10] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), SPECIAL PUBLICATION 1191: RESEARCH ROADMAP FOR SMART FIRE FIGHTING (May 2015), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1191.pdf.

[11] NIST, Cyber-Physical Systems Homepage, http://www.nist.gov/cps/ (last visited May 23, 2016).

[12] *See, e.g., Comment of Nest Labs, Inc. on U.S. Environmental Protection Agency's "Federal Plan Requirements for Greenhouse Gas Emissions From Electric Utility Generating Units Constructed on or Before January 8, 2014,"* Docket ID Number EPA-HQ-OAR-2015-0199; FRL 9930-67-OAR (January 21, 2016) (describing the potential for smart thermostats and other advanced home energy controls to yield significant energy savings and contribute to US greenhouse gas emission reduction efforts); *Comments of Nest Labs, Inc. on Southern California Edison Company's Proposal in Response to Assigned Commissioner's Ruling Directing Activities in Response to Natural Gas Leak at Aliso Canyon Storage*, Rulemaking 13-09-011 (Cal. P.U.C. Sept. 19, 2013) (noting the potential for smart thermostats to assist in mitigating the effects of the natural gas shortage caused by a leak at the Aliso Canyon Storage Facility).

benefits, and potential harms that new connected device technologies will bring. Technology will evolve in beneficial, but as-yet unanticipated directions, and Nest respectfully submits that public policy, as a general matter, should accord it the space to do so, subject, of course, to the full range of consumer protection laws and other protections that are already in place to address concrete and observable harms.

- *Fourth*, the Department should help regulators at all levels remain appropriately cautious of seemingly benign rules that entrench lower-functioning products or are not technology-neutral. As one example, well-intended legislative proposals to mandate specific power source requirements for battery-powered smoke alarms effectively preclude connected alternatives from the market notwithstanding the substantial benefits of those devices. As the FTC has recognized in other contexts, technology-specific mandates can have unintended exclusionary effects on newer, innovative technologies to the detriment of consumers and market competition.[13] Nest of course respects the right of individual states to regulate within their own borders. However, Nest respectfully suggests that both state and federal policymakers consider the risks of imposing potentially inconsistent or overly specific technical mandates, which can impede the development of new technologies and have spillover effects across jurisdictions.[14]

- *Fifth,* government should allow private actors to determine the standards that will allow IoT technologies to reach their potential, recognizing that that process may

[13] *Cf.* Note by United States (submitted by Federal Trade Commission), OECD Hearing on Disruptive Innovation, Directorate For Financial And Enterprise Affairs Competition Committee (June 19, 2015) ("Incumbent firms sometimes attempt to use the existing regulatory process to make it more difficult for new products, services, and business models to compete by encouraging regulators to amend existing regulations to more explicitly cover the innovative product, service, or business model or to put in place regulations with which new businesses cannot comply . . . . This can potentially undermine the achievement of safety, consumer protection or other public policy goals, while disadvantaging incumbent firms who continue to be subject to existing regulations."), *available at* https://www.ftc.gov/system/files/attachments/us-submissions-oecd-other-international-competition-fora/1507disruptive_innovation_us.pdf.

[14] *Cf., e.g.*, FED. TRADE COMM., FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (Feb. 2009) (supporting industry self-regulation in the area of online behavioral advertising "because it provides the necessary flexibility to address evolving online business models."). Consistent with the principle of letting the market sort out winning and losing technologies, some products will find a long-term audience and others will not. When it becomes necessary for a product or service to exit the market, companies should endeavor to avoid or minimize disruption to their customers; likewise, governments should recognize that sometimes such decisions are inevitable and accord companies room to determine how best to communicate with their customers and effectuate responsible shutdown planning.

take some time. Consumers will realize the full benefits of residential IoT only when all the devices in a home can speak to one another in a common language. As one example, Nest has heavily invested in its Works with Nest program, which enables third party developers to build integrations with Nest products. Multiple protocols exist, of course, and the evolution of common standards can greatly aid in building interoperability. This evolution will occur organically, as it has in other contexts. In the meantime, governments should encourage voluntary collaboration while allowing the private sector appropriate space to develop solutions rather than mandating coalescence around any specific protocols.

IV. The Existing Robust Legal Framework for IoT

The current legal framework governing IoT devices provides strong safeguards for consumers and the flexibility to adapt to new technologies and business models.

At the federal level, the FTC Act's prohibitions on deceptive and unfair practices are the bedrock of consumer protection.[15] This authority empowers the FTC to address a broad range of consumer protection issues that may arise through IoT technology. The FTC has a strong track record of using its Section 5 authority to ensure that companies respect consumer privacy, keep data secure, and adhere to established consumer protection principles in deploying new technologies.[16] Significantly, the FTC has demonstrated a keen interest in IoT, already bringing several enforcement actions with regard to connected consumer devices even though the industry is still in its infancy.[17] The FTC has also been vocal in encouraging best practices for IoT companies, holding a workshop that brought together a variety of stakeholders, and issuing an influential report setting forth key privacy and security practices for IoT.[18] Nest commends the FTC for its active role with respect to IoT, which encourages industry to adopt best practices and recognize the importance of consumer protection issues.

---

[15] *See* 15 U.S.C. § 45(a)(1).
[16] *See, e.g.*, Fed. Trade Comm., *2014 Privacy and Data Security Update*, *available at* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.
[17] *See ASUSTeK Computer, Inc.*, FTC File No. 142-3156, Proposed Compl. and Consent Order (Feb. 26, 2016); *TRENDnet, Inc.*, No. C-4426, Compl. and Decision & Order (Feb. 7, 2014).
[18] FED. TRADE COMM., INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf ("FTC IoT Report").

Most states prohibit unfair and deceptive practices under laws similar to Section 5 of the FTC Act, and state attorneys general and private plaintiffs have provided an additional mechanism to enforce these prohibitions.[19] States also have robust data security and digital privacy laws, including laws requiring companies to notify consumers in the event of data breach,[20] laws that impose specific data security requirements,[21] and laws that impose specific data use and disclosure requirements, such as California's Online Privacy Protection Act.[22] In addition to Section 5 of the FTC Act, an array of specific federal and state laws regulate specific harms that can arise in contexts including, but not limited to, IoT. For instance:

- A host of federal product safety laws, including the Consumer Product Safety Act[23] and the Federal Hazardous Substances Act[24] (with precise application depending upon the technologies and materials incorporated within a device) impose stringent safety requirements on IoT devices.

- The Wiretap Act restricts the recording of private communications without consent,[25] and the Computer Fraud and Abuse Act prevents access to a computing device without authorization from the owner.[26]

- Many states have laws prohibiting oral recordings without the consent of all parties to a conversation, as well as videotaping people in places where they have a reasonable expectation of privacy.[27]

- The Children's Online Privacy Protection Act and implementing regulations restrict the collection, use, and disclosure of personal information from children

---

[19] *See, e.g.*, Cal. Bus. & Prof. Code § 17200; Md. Code Comm. Law § 13-301; § 13-303; Md. Code Comm. Law § 13-303 (unfair practices); *see also* Maryland Office of the Attorney General, *Attorney General Gansler Forms Internet Privacy Unit* (Jan. 28, 2013), *available at* https://www.oag.state.md.us/Press/2013/012813.html; State of California Department of Justice, Office of the Attorney General, *Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit* (July 19, 2012), *available at* https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection.

[20] *See, e.g.*, Cal. Civ. Code § 1798.80 *et seq.*; N.Y. Gen. Bus. Law § 899-aa; 815 Ill. Comp. Stat. 530.

[21] *See, e.g.*, 201 C.M.R. § 17.

[22] Cal. Bus. & Prof. Code § 22575 *et seq.*

[23] 15 U.S.C. § 2051 *et seq.*

[24] 15 U.S.C. § 1261 *et seq.*

[25] 18 U.S.C. § 2510 *et seq.*

[26] 18 U.S.C. § 1030.

[27] *See, e.g.*, Cal. Penal Code § 632; Del. Crim. Code, tit. 11 § 1335; Ill. Ann. Stat. 720 ILCS 5/14.

through Internet-connected services and through online services that are directed to children.[28]

- The Fair Credit Reporting Act imposes strict limitations on the use or disclosure of information for purposes of determining an individual's eligibility for credit, insurance, or employment, ensuring that consumers have visibility into and control over the data that is used to determine their eligibility for crucial benefits.[29]

- The Video Privacy Protection Act limits disclosure and storage of information about individuals' video viewing habits.[30]

This overlay of existing law provides a significant bulwark against concrete harms that have been encountered and regulated over a period of many years, refined through a gradual process of case law development. Accordingly, as new technologies like IoT develop, they do so against a well-established backdrop of legal protections. In light of this existing backdrop, Nest agrees with the FTC's recommendation that IoT-specific legislation would be premature at this time.[31] Indeed, such legislation could risk inhibiting the incredible potential for innovation in this area.

V. Privacy and Security

A. Data Enables Many of the Benefits of IoT

Many of the benefits provided by IoT technologies come from their ability to gather data from their environments, to receive and respond to inputs, both local and remote, and to apply data in thoughtful ways. For example, the Nest Learning Thermostat can employ motion sensing and smartphone geofencing to determine when a house is empty, enabling it to adjust the temperature and save consumers money on their heating and cooling bills.

Data collected by IoT devices can also be used to help them continue to function properly after installation. It can enable devices to "learn" and improve to suit their

---

[28] 15 U.S.C. § 6501 *et seq.*; 16 C.F.R. § 312.
[29] 15 U.S.C. § 1681 *et seq.*; 12 C.F.R. § 1022.
[30] 18 U.S.C. § 2710 *et seq.*
[31] *See* FTC IoT Report, *supra* note 20, at 48-49 ("Staff agrees with those commenters who stated that there is great potential for innovation in this area, and that legislation aimed specifically at the IoT at this stage would be premature.").

owners' preferences (for example, temperature preferences at different times of day). And it can enable companies to develop new features so that products and services get better over time. As an example of this, Nest used data from Nest Protect to develop the Steam Check feature, which helps to reduce the incidence of nuisance smoke alarms caused by steam.[32] Nest analyzed trends in the characteristics of steam-generated alarm events and the differences between steam- and smoke-based events. Using these data, Nest developed a software algorithm to help distinguish between steam- and smoke-based events and reduce the nuisance alarms from steam (such as a shower), without impairing proper operation of the alarm in case of an actual smoke or fire event.[33] Because Nest Protect is Wi-Fi equipped, Nest was able to make this feature (which can be turned off or on at the user's preference) available through an automatic software update to installed alarms, so our customers could receive the benefit of Steam Check without needing to purchase new hardware.

B. Privacy and Data Security are Crucial to IoT

At Nest, we believe that home is a sacred space and our products are invited guests. Earning and keeping our users' trust is fundamental to our success as a business. As a result, we strive every day to uphold that trust by establishing and honoring clear privacy commitments, respecting our users' privacy preferences, and working diligently to secure the data we collect.[34]

Likewise, the long-term success of residential IoT will depend on companies earning and maintaining consumer trust.[35] It is important for manufacturers and service providers to remain cognizant that collection, use, and maintenance of many types of data from the home can be sensitive. Companies should have discretion to determine the appropriate methods and types of notice to provide in order to ensure that there is a meaningful foundation of customer consent, and in emergent product categories such

---

[32] Nest, *What is Steam Check?*, https://nest.com/support/article/What-is-Steam-Check (last visited May 25, 2016).

[33] NEST LABS, NEST PROTECT STEAM CHECK STUDY: RESULTS FROM NOVEMBER 2013 TO MAY 2014 (Sept. 2014), *available at* https://s3.amazonaws.com/support-assets.nest.com/images/tpzimages/tpz-steam-check-white-paper.pdf.

[34] Nest endeavors to be transparent and vocal about these principles, stating them clearly on a privacy page on its website. *See* Nest Labs, *Privacy Statement for Nest Products and Services* (last revised Mar. 10, 2016), *available at* https://nest.com/legal/privacy-statement-for-nest-products-and-services/.

[35] *See, e.g.*, FTC Chairwoman Edith Ramirez, *Opening Remarks of FTC Chairwoman Edith Ramirez Privacy and the IoT: Navigating Policy Issues International Consumer Electronics Show* (Jan. 6, 2015) ("trust is as important to the widespread consumer adoption of new IoT products and services as a network connection is to the functionality of an IoT device"), *available at* https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf.

as those enabled by residential IoT they may find novel ways to do this. Mechanisms for providing notice and obtaining consent may reflect these changes, and government should be cautious of over-prescribing specific implementations. At the same time, it is essential for companies to take their customers' privacy and security seriously, be transparent about the collection and use of data from the home, and ensure that they are respecting customers' preferences.

1. Privacy and Residential IoT

In residential IoT, products are generally invited into the home by consumers. This implies a degree of intentionality on the part of consumers, who have chosen to use such products (instead of more conventional, non-connected alternatives). In order to help ensure that consumers can make informed decisions about what devices to allow into their homes, companies should strive to provide clear disclosures on what data is being collected by their devices, and how it may be used. At the same time, providing this information can present practical challenges, as the FTC has recognized.[36] Discussion of privacy in the context of IoT should recognize that many connected home devices do not have an integrated display, such as screens or other user interface, on which privacy notices or choices can be provided. On the other hand, connected devices may offer possibilities for notice that conventional, non-connected products lack, such as in-app notifications.

Manufacturers of connected devices should be innovative in working to educate their customers about the data practices of their devices in light of the absence of a screen or similar user interface. At the same time, regulators should be cognizant that these inherent limitations need not undermine confidence in the prospect of in-home sensing and automation generally. Rather, regulators should provide companies with appropriate latitude to develop and employ practicable, effective methods of informing their customers of their practices, while not unduly impeding the deployment of new technologies. Recent progress toward electronic labelling, for example, is a welcome development and should be encouraged and expanded.[37]

For its part, in addition to its long-form privacy policy, Nest provides notice where appropriate through the Nest mobile application, a tool that enables some of Nest's advanced capabilities (such as video, remote temperature adjustment, and the ability to

[36] *See* FTC IoT Report, *supra* note 20, at 39 ("While the traditional methods of providing consumers with disclosures and choices may need to be modified as new business models continue to emerge, staff believes that providing notice and choice remains important.").
[37] *See* E-Label Act, Public Law 113-197 (2014).

silence a smoke alarm without climbing onto a ladder to manually hush the device). We also provide notice through a dedicated, easy-to-understand and user-friendly privacy page (nest.com/privacy), our more detailed privacy policy on the Nest website, and through product packaging and in-box materials.

Nest also commits to obtain user consent before sharing personal data with third parties who do not act as service providers. We make clear that "we will ask [our users'] permission before sharing [their] personal information with third parties for purposes other than at [our users'] request or to provide Nest's Products."[38] Moreover, we do so "only when we think [such third parties] will provide [users] with a welcome additional service," and we commit to "not rent or sell our customer lists."[39] One example of this occurs during the Works with Nest enrollment process, which is where customers initiate the connection of Nest products with third-party products in the Nest app or via the Works with Nest website. Nest requests consent to share data with a third-party developer by not only telling customers what information will be shared but also by providing commentary from the third party on why that information is being requested and how it will benefit the customer.

We recognize that other companies may employ different business models and means of providing notice. They may also choose a different set of commitments for their customers. What is vital is that they articulate a set of responsible commitments and adhere to them. Especially for a sacred space like the home, earning and maintaining user trust is fundamental.

2. Data Security and Residential IoT

Adopting and maintaining reasonable and appropriate protections to secure data from unauthorized access is also critical to earning and keeping user trust. While the security risks associated with different product categories can vary, manufacturers of connected products in the home must take security seriously and endeavor to implement responsible security measures from product design onward. As interconnected networks of devices spring up, companies should remain appropriately vigilant to avoid inadvertently introducing a security vulnerability that gives attackers easy access to an otherwise well-secured smart home network. The resiliency of in-home mesh networks can be a tremendous strength, and should be encouraged. At the

[38] *See* Nest Privacy Statement, *supra* note 36.
[39] *See id.*

same time, companies should recognize the importance of implementing responsible security measures particularly in such interconnected environments.

There are other steps that companies can take to help build security into the IoT. These include "security by design" — building security into their products from an early stage rather than as an afterthought; testing security measures before launch; participating in bug bounty programs; educating consumers about security features; and taking meaningful steps to inform consumers when security updates are available. Nest applauds the work the FTC is doing to build awareness of the importance of security to the success of IoT, as it is important for IoT manufacturers to have a clear set of principles or guideposts for which they can aim. We encourage the FTC to expand its existing efforts to educate industry on what the FTC considers to be reasonable and appropriate security for connected devices. Clarity and certainty as to regulators' expectations will encourage IoT manufacturers to adopt sound and responsible practices without fear of retroactive liability based on unclear substantive legal standards.

Likewise, the Department could play a productive role by encouraging providers of connected devices and associated services voluntarily to provide more information about their security practices in the public domain. This is not to suggest mandating specific technical measures or expecting companies to publicize confidential or proprietary information or information that could be exploited by malicious actors, but rather to suggest that basic disclosure about a company's security efforts (for example, the fact that a company encrypts data at rest and in transit, its authentication measures, and its use of vulnerability testing) could help promote responsible security practices across the IoT.

VI. Promoting the Cross-Border Flow of Products and Services

Nest appreciates the Department's work in helping to ensure that technology companies, including IoT companies, can make their products and services available across borders. For instance, the Department's efforts to negotiate an alternative to the U.S.-EU Safe Harbor Framework after the European Court of Justice's decision in *Schrems v. Data Protection Commissioner*[40] helps ensure that companies can transfer data across borders with legal certainty to the benefit of businesses and consumers on both sides of the Atlantic. Without this free flow of data, innovation would suffer;

[40] *Schrems v. Data Protection Commissioner*, No. C-362/14, [2015] ECR, *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en.

mandatory data localization laws and similar barriers to trade threaten to hinder the growth of IoT to the detriment of consumers, businesses, and society at large. Nest urges the Department to continue its efforts to ensure that data can continue to move freely across borders. In addition, we encourage the Department and the FTC to invest the resources necessary to make the new Privacy Shield a success.

In addition, Nest respectfully encourages the Department to work with other governments and multinational institutions to promote regulatory consistency in consumers' best interests across international borders. Inconsistent rules or technical specifications that don't clearly benefit consumers or companies can significantly impair IoT companies' ability to expand internationally, or force them to expend significant resources re-engineering their products to achieve compliance without commensurate user benefit.

VII. Conclusion

Just as the Internet is yielding extraordinary benefits for consumers and the economy, connected technologies have the potential to generate extraordinary benefits. Adopting a pro-innovation posture, encouraging responsible privacy and security practices, and helping to promote a vibrant cross-border flow of products and services can all help in realizing these benefits. To that end, Nest appreciates the opportunity to comment on IoT and stands ready to work with NTIA and other stakeholders on these important issues.

Respectfully submitted,

J. Scott Kohler
Counsel, Product & Regulatory
Nest Labs, Inc.