OPEN IDENTITY EXCHANGE

Setting a Comfort Zone For Privacy in the Internet of Things

The Smart Thermostat Use Case

White Paper

by: Scott L. David

Setting a Comfort Zone For Privacy in the Internet of Things: The Smart Thermostat Use Case

Executive Summary: The Internet of Things has created a new category of products defined by their ability to input and withdraw data to and from networks of related products. One product typifies such new uses of network connectivity: The smart thermostat. This paper will examine the benefits and challenges of smart thermostats and the Internet of Things. This paper highlights the benefits to individuals of these systems such as: comfort, convenience, choice, efficacy, self-knowledge, value realization, and security. By isolating these benefits, we hope to establish a benefits-based framework for the creation of new products in the Internet of Things. The Internet of Things will also address many of the issues revolving around privacy concerns with data. Unpacking these benefits will demonstrate the value of applying the Internet of Things to everyday products.

I. Introduction

a. Thermostats as IoT

This paper explores smart thermostats as an instance of the Internet of Things (IoT), a system of connecting once-isolated things, with a focus on how IoT can offer new benefits to individuals. The focus on individual benefits of IoT is prompted by recognition that the perception and reality of such benefits to individuals (acting in both institutional and non-institutional settings) is foundational to successful adoption of new technology, particularly in consumer-facing deployments of IoT.

Smart thermostats are connected to the Internet so that data that has been collected for use in systems operations can be retained, and has the potential for additional valuable use. When commercial and governmental institutions that rely on data flows generated by individuals are able to create and deliver IoT systems that can be demonstrated to reliably, predictably and consistently deliver the types of benefits described below, they will witness adoption curves that exceed those evidenced in the current market for data and identity-related products. They will enjoy and foster monetary and other value enhancement resulting from increases in data volumes prompted by pursuit of such benefits by individuals.

Some of those individual benefits will be derived from IoT enhancements of existing technology (such as augmented thermostat function to enable remote temperature adjustment), while other individual benefits will be entirely new ones associated with the handling and use of IoT data itself (such as new data management services that offer data leverage and risk reduction to individuals). Each benefit will be accompanied by different promises made by service providers and different metrics to gauge their performance against such promises. In both cases, the ability of an organization to demonstrate that promises made are promises kept is a precursor of trust in distributed systems such as the Internet, and is also handy shorthand for compliance advice.[1]

This paper takes the viewpoint of individuals, and suggests that the analysis of their benefits is a prerequisite to identifying metrics associated with those benefits, and a pathway to enhanced adoption of IoT. The definition, audit, and valuation of the performance of data and identity systems against such standard metrics will enable commercial and governmental institutions to develop and deploy scalable systems to govern IoT.

[1] See, e.g., U.S. Federal Trade Commission Media Report at http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.

These loosely coupled structures of governance will initially resemble traditional "supply chains," reflecting the underlying distributed structure of the Internet that is the object of such governance. Such governance will be grounded in and made coherent by the identification and adoption of shared metrics that help stakeholders to simultaneously weigh the benefits to themselves and others of various data actions and the related costs and burdens of those actions, and to evaluate the performance of systems from which the benefits are derived. The overall structures of that governance will be discernable by the plotting of those metrics on a relationship "map" of interrelated benefits and burdens; of rights and duties that can help to inform the design, development, and deployment of IoT systems.

Thus, this paper seeks to present not just a catalog of emerging benefits and challenges, but also the beginnings of a virtual "map" of the IoT risk and benefit territory to inform systems engineering of these socio-technical systems. This exercise suggests that applying an initial "benefits cartography" can help to get the attention of stakeholders. Once started, the benefits "map" can then be made more comprehensive and precise through incorporation of benefits to institutions (which is deferred in this paper), and by the natural operation of people acting together to perform the collective "benefits triage" that takes place by applying the lenses of institutions such as markets, governments and cultural structures.

These localized efforts will naturally be brought together in markets operating at multiple levels to surface various "best practices" for achieving such benefits. The desire of stakeholders to compare trust framework offerings will, in turn, drive the development of registries. The registries will offer stakeholders interface with multiple overlapping trust frameworks that can be readily surveyed and analyzed in various stakeholder solution-seeking contexts. The pendency of this developmental narrative is confirmed by the various user-centric rulemaking efforts based on individual benefit that are already underway, albeit with different procedural bases, through different regulatory and self-regulatory initiatives worldwide.

b. A "benefits-based" analytical framework

Empathy and altruism are desirable human traits, but ones that have not been historically demonstrated to be reliably ascendant in predicting the collective behavior of human populations, particularly where populations are isolated from one another (whether due to divisions of geography, lack of consanguinity, language, culture, etc.). Distance enables abstraction and its consequent callousness and the "violence" of externalization of costs imposed on populations on the receiving end of "NIMBYism." The distributed structure of the Internet creates relationship distance and the setting for such abstraction, callousness, and "violence" to manifest in its many forms (such as the violence of externalizing costs and harms to other people at the edges of various benefits "bell curves").

The IoT creates an intimacy of engagement that can foster architectures of empathy from hybridizing altruistic and self-interested behavior. When people recognize their dependency on the behavior of others (such as regarding their data handling practices), they are more likely to behave with attention to the interests of others, with the hope that their good example will encourage others to act similarly. It is not unlike initiatives to encourage individual hand washing habits during flu season, the broad adoption of which confers both individual and "herd" immunity. This manifests a more reliable form of empathy born from self-interest which could be captured in an individual declaration of interdependence; a "golden rule" for data: "I will do unto data about others as I would have them do unto data about me," reflecting both an aspiration and a warning regarding data behaviors. If performance of this promise is made measurable, it can be enforceable, enhancing system reliability.

Such a "golden rule of data" is an example of the concept of "mutual" or "reciprocal" altruism that was originally proposed by evolutionary biologist Robert Trivers, which tweaks altruism to include an element of self-interest that may be a more reliable predictor of behavior. The concept, which also pops up in game theory, is that people often act in ways that benefit others with the "soft" expectation of indirect or delayed personal benefit from others acting similarly. Enforcement reduces "free riders" and can convert that hope to a more reliable expectation. This paper suggests that the "trust" that is sought to be established for IoT and other scaled data and identity systems, can be built on the "reliability" of self-interested behavior of stakeholders in structures where that behavior is woven into a social economic, political and cultural tapestry of interdependency through which each stakeholder recognizes the accomplishment of their respective benefits to be mutually dependent on their performance of behaviors that in turn help to realize the benefits to other stakeholders. Networked data systems enable individual benefits that cannot be realized by individuals acting unilaterally, and enforcement of network-stabilizing behaviors can be promoted by withholding those benefits from negligent and bad actors. This is not new; in fact it is the ultimate source of authority from which all social structures ultimately are grounded.

Mutual altruism anticipates a rough accounting of benefits provided and received, with "free riders" (who take more than they provide to the system) ultimately subject to group sanctions. This "tit for tat" balancing is reflected in all governance structures to which individuals voluntarily commit themselves. However, the new challenge is to contemplate how such relationship structures can be accomplished in the massively distributed Internet in which IoT will be integrated, where the system exceeds the boundary of any compulsory authority such as a single sovereign nation or a commercial entity, which could otherwise compel observance of the golden rule of data. What is the nectar that can incentivize the massive data cross-pollination to yield the fruits of big data for all stakeholders? IoT increases the urgency of such contemplation, and provides the incentive for parties to participate. The various proposals for online "reputation based" systems provide a

glimpse of future mutual altruism accounting structures for future distributed governance. The source of the problems is also the source of the solutions.

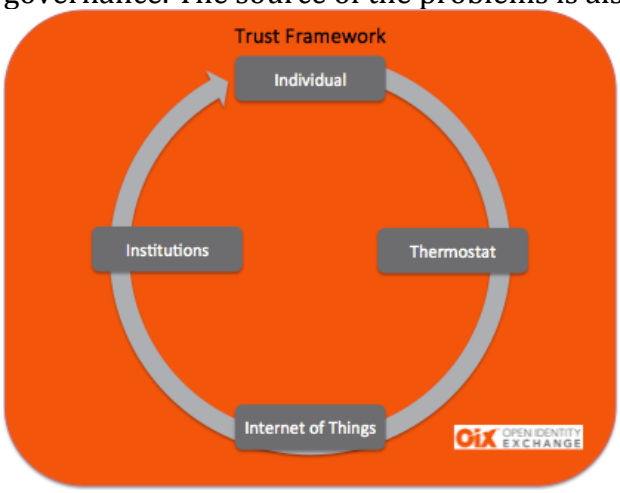

Figure I-1: Benefits Relationship

Figure I-1 depicts the interdependence of the relationships in the general trust framework this paper hopes to illustrate. When data from a closed system, such as a home thermostat is shared beyond the heating system of the individual user in the co-managed structures of the IoT, its broader use generates value for all stakeholders including structures of benefits to individuals, and provides individuals with greater efficacy to dynamically communicate their evolving needs in areas such as privacy, security and benefit realization through their participation in valuable information supply chains that feedback into stable, sustainable relationship loops..

II. Individual Benefits

This section examines some of the specific benefits to individuals of IoT-related enhancements to thermostat function as a benefits-focused framework for exposing the role of IoT both as a source of functional augmentation of traditional (pre-IoT) physical systems, and more broadly as a source of stand-alone leveraged value from the informative insights gleaned from managed secondary uses of data about systems inputs, outputs, performance, and comparisons. In other words, how does IoT affect thermostat function, and vice versa?

IoT can be most effectively and comprehensively examined simultaneously from multiple perspectives, embracing the complexity of the many decisions that inform all stakeholders' specific adoption decisions for IoT-related technologies. People and institutions weigh a host of different variables in making decisions, including IoT-related participation and consumption decisions.

Those decisions can be informed both by objectively-measured variables (such as monetary costs, time and effort costs, and some security issues, etc.) and also by a variety of subjective factors (such as values, norms, cultural preferences, ethical considerations, privacy concerns, and some other security issues, etc.), making generalization and comparison of influences on decision making across populations both difficult and potentially misleading.

Notwithstanding the challenges, this paper suggests that, in considering the strategies for facilitating stakeholder adoption of IoT-based products and services, it is initially helpful to parse the analyses based on the general types of benefits to individuals (some of which are listed below in this section II), since IoT deployments that can deliver measurable, reliable benefits to individuals will achieve massive scales (and the benefits of scaling and network effects) in consumer-facing contexts. Many categories of "individual" benefits (such as security, convenience, etc.) are also relevant in institutional settings where individuals (as employees) make decisions about IoT adoption and deployment. Even when people are acting on behalf of institutions (such as companies or governments), such human benefit factors can strongly affect employee and contractor acceptance of IoT deployments and their adoption curves, and can lower education and other conversion costs. This discussion is organized based on categories of individual benefit to help identify adoption-enhancing strategies for IoT.

The categories of individual benefits of smart thermostats include (but are not limited to): (i) greater personal comfort and health, (ii) more convenience, (iii) enhanced choice, (iv) greater self-knowledge, (v) greater value realization, and (vi) greater security. These are each described below. The seventh benefit of "privacy" that has become synonymous with multiple individual benefits in a networked world is discussed in a separate section (Section III) that predicts that the data

deluge of IoT will usher in the possibility of sustainable privacy in a hyper-networked world beyond secrecy.

This paper also suggests that consideration be given to further analytical divisions within each of the seven benefit categories based on one of three potential technology system sources each reflecting the relative importance of ever greater levels of interactions and relationships (and the value of information that powers those relationships), from isolated systems to ICT-enhanced systems, through a fully matured IoT ecosystem. The three sources are specifically identified as (i) traditional (local) thermostats, (ii) thermostats enhanced with closed data systems, and (iii) thermostats networked into more expansive information systems. The separate treatment of these three distinct benefit sources is intended to help tease out those benefits that accrue from each category of technology, revealing new benefits that can arise only through network participation.

From a practical perspective, this framework is also intended as a system trust framework design tool to aid in the consideration and creation of structures of incentives and penalties based on the five categories of benefit to support reliable, predictable and sustainable IoT deployments, with IoT thermostat deployments providing the current example. The framework of this section (6 benefits and 3 sources) yields 18 potential individual benefits "states" to consider in the trust framework construction and evaluation contexts. Structuring of interdependent stakeholder benefits is the foundation for trust frameworks and the future data and identity rights markets that they will convene.

This analytical framework is thought to be potentially helpful since it may help distinguish stronger from weaker source of influence (through structures of benefits offering incentives where possible and penalties where necessary) in individual and institutional decision making among different stakeholders involved in IoT, and to foster greater "cross talk" among stakeholders engaged in IoT design, development and deployment contexts. The separate brief analyses of three sources within each benefit category will also help to reveal the types of trade-offs that all technologies invite us to make in the course of their adoption, i.e., enhanced leverage and risk reduction in some areas, paid for by greater dependency on the technology, greater standardization, and new risk profiles.

The "benefits framework" is intended to identify the types of "nectar" that will attract stakeholders who then help to pollinate the system yielding fruitful information. IoT is a socio-technical system that depends on the reliable behavior of technology and people to succeed. The Internet has come to serve as an economic, political, educational, social and cultural crossroads. The reason for focusing on the Internet's social nature is that its stability and reliability is no longer simply a matter of technical standards and fixes. Rather, it requires socio-technical solutions for sociotechnical problems. The identification of stakeholder benefits is a prerequisite to the construction of incentives and penalties for this system to draw

stakeholders to self-bind to enforceable promises regarding data actions that collectively generate maximum benefits to all stakeholders.

Reliable technology and reliable people and institutions are at the core of trusted systems. Reliable technology is fostered (and evaluated) by conformity to standard specifications. Reliable people and institutions are encouraged by the policies that structure the incentives and penalties of benefits provided or withheld to foster the habituation of system-friendly behavior by such individuals. This section explores those benefits as the "quanta" of stakeholder decision-making.

The IoT concept generally implies the bringing together of networked data infrastructure with a variety of physical infrastructure with which we already interact. This merging of various physical and information "feedback loops" will have different leverage and risk implications for each system that is brought "online" into the IoT; and the analysis will also be different for each stakeholder depending on their subjective needs and context. The higher-level interactions of these multiple relationship "loops" are complex, but until they are "mapped," (such as in trust frameworks and registries) no stakeholder can make fully informed decisions, and none will realize the full benefits.

This benefits-centric mapping is intended to highlight some of the interests and concerns of individuals to help shift the discussion from "agenda setting" to "problem identification" in the parlance of Ronit and Porter.[2] Applying their 5-stage construction of rulemaking to this paper's benefit framework, the expected benefits (revealed in Stage 1 "Agenda Setting"), such as those listed below, become a system reliability "problem" if they are not delivered. Relevant metrics for such identified stakeholder problems (the focus of Stage 2 "Problem Identification") help to guide the current discussion in multiple initiatives in various jurisdictions and sectors of candidate sets of rules "decisions" (Stage 3) and "implementation" strategies (Stage 4) for maximum impact to stakeholders. Those metrics also enable feedback systems (through such mechanisms as markets, independent audits, etc.) to "evaluate" (Stage 5) and dynamically mature the stakeholder-derived rules system among benefitted and burdened parties. As IoT achieves increasingly pervasive deployment, their 5-stage model can be applied as a framework for each level of nested data rights service development that overall reflects self-regulation in myriad communities of interest of data rights at Internet scales.

a. Personal comfort and health

i. Traditional Thermostats

Since the late 1800's, electric thermostats have been used in residences to help maintain comfortable temperatures, and even before that, they were used in incubators to protect the health of poultry.

[2] See, Tony Porter and Karsten Ronit, "Self-regulation as policy process: The multiple and criss-crossing stages of private rule-making, (Springer, 2006).

Thermostats are sensors that are part of "closed" feedback systems that control the deployment of HVAC systems in ways that link ambient temperature to a user's temperature preferences. The systems are "closed" since the data that is generated by the operation of the sensors in the thermostat (i.e., the user's settings and the ambient temperature), and by the operation of the heating source is only used within the system. Historically, the closed feedback system of HVAC was sufficient to satisfy the personal comfort needs of the user.

ii. Data-Enhanced Thermostats

Thermostats clearly rely on data for their operation even within the closed feedback loops of stand-alone HVAC systems described above. As lifestyles have taken family members increasingly out of the home, and as information communication technology (ICT) capacities and price points have enabled remote communication with home systems, there has been increasing demand and capability to provide access to remote control of home functions, such as controlling lights for security, controlling heat for cost savings, monitoring water for flooding, monitoring entries for burglary, etc. Each of these systems extends the data flow of its respective "control system" beyond the home for the enhanced comfort and safety of system users. These systems might still be called "closed" since the HVAC user still has exclusive access to the system data, even though not present at the site where the system operates.

In some cases, off-site, third party monitoring services (such as home security against theft or fire, freeze alarms, etc.) are offered so that users can have the leverage advantages and comfort of knowing someone else is also monitoring system performance on their behalf. The party monitoring such systems has historically been understood to be engaged in the service solely on behalf of the service user. However, the precise status of such monitoring has not been fully developed since the data risks were historically low. The data that they monitored was relatively limited, and was not broadly networked. Such monitored systems might be called "semi-closed" since a third party is brought in the loop by adding ICT capacity to the system, but is still acting solely or primarily for the system user.

iii. Networked Thermostats

Data (such as a thermostat's setting at a particular time of day) that has been referenced by the system for its immediate operations (such as primary use in control systems for heating) can also have value as information beyond those operations. In fact, such data might be used with other data in a variety of managed; secondary ways beyond its initial function, without negatively affecting its primary use or system users, but the potential for such harm exists. Such "secondary" use is frequently what is hinted at by the term "big data," the matured form of which is broadly anticipated to achieve both leverage and risk reduction (including privacy risk reduction). This paper suggests that the IoT can be built and sustainably maintained to balance stakeholder needs.

Traditional thermostats did not typically include the capacity to "store" data (except, of course, to the extent that user settings remained fixed until changed by the user). Data regarding elements of thermostat use and operation can, however, have value to system users in recording prior system performance to inform future decisions (such as energy system consumption and operation decisions – for example the cost effectiveness of installing extra insulation). The same data can also have value to third parties such as in the analysis by energy producers and distributors in energy and equipment supply chains, and in informing social issues such as energy consumption and climate change.

b. Convenience

i. Traditional Thermostats

Thermostats vastly increased human convenience, as anyone who ever lived without one in a wood-stove-heated dwelling can confirm. Humans can survive without technology, such as ambient temperature control technologies, but not as comfortably – and certainly not as conveniently. Our external physical and informational environments are highly mediated by technology to make life more convenient, pleasant and productive, but at the cost of our becoming less habituated to, and functional in, unmediated settings.

ii. Data-Enhanced Thermostats

The extension of IoT to thermostats and other home systems has already enabled tremendous new services to users to further enhance their convenience. Remote monitoring and control of heating and cooling offers the convenience of system control wherever a user is located; through a sort of narrow-band "telepresence." Now people can control their thermostats remotely to maximize their comfort and convenience, while minimizing cost.

iii. Networked Thermostats

IoT increases consumer convenience by connecting individual thermal related comfort needs to potential solutions for enhanced convenience. By connecting a thermostat to the broader IoT, data from one system can be compared to that of other similar systems deployed in similar settings to reveal opportunities for consumers to discover convenience-enhancing strategies of similarly situated individuals. For example, a consumer might discover a remote system for making sure that their remote dependents' (e.g., aging parents in another state) HVAC systems are functioning properly in periods of extreme temperatures, without having to visit, or might learn that shades should be opened on the south side of a home in the morning and closed in the evening in winter to maximize solar heat gain.

c. Individual choice

i. Traditional Thermostats

Traditional thermostats offered users choice of ambient temperature controls that required little or no maintenance (unlike a wood-fired stove, e.g.). The nature of the

choices made available to thermostat users is constrained by the limited number of interactions and measurements needed for HVAC system function. In "bang bang" thermostat operation (i.e., the absence of a "proportional response," so that the system turns on fully in response to a call for heat, and then off fully when the thermostat indicates that temperature is reached), few datum are required for system operation.

ii. Data-Enhanced Thermostats

With the advent of remote access to HVAC systems, users' choices expanded. For the first time, users were offered choice regarding the place in which they interacted with their HVAC systems' controls. Many systems also developed programmable features, such as synchronizing HVAC function with time data, which offered users greater choice of system programming function.

iii. Networked Thermostats

IoT offers fundamentally different insights into systems operation than is available with stand-alone systems, enhancing user choice. With IoT, the data from multiple systems' operation can be collected, compared and analyzed as a group. This can be done by third parties, or more privately by apps designed to minimally intrude on the user. As a result, IoT opens up the possibility of greater choice in terms of "information seeking" behaviors of users, the cost of which to the user is providing access to information that can feed the information seeking behavior of one's neighbors.

The ability to compare system performance data to that of other systems vastly increases consumer choice by expanding the range of considerations that inform individual consumption decisions such as heating system design, construction and operation. Networked HVAC data also opens up the possibility of many more interactions involving such data, and greater volume of interactions yields greater opportunities for consumer choice. Personal innovation can be enabled by better information made available through participation in IoT. As is discussed in section III on "privacy" below, however, risk also increases with interaction volume.

IoT will also constrain choice in some ways by virtue of the need for standards that enable leverage and risk reduction for stakeholders at large scale. In sociotechnical systems, one party's reliability is another's constraint. Choices of users in all large networks are constrained in various ways by standards. Consider that HVAC relies on standardized electricity networks that only provide service at one voltage (120v in U.S.), oil is available only as standard heating or stove oil, gas heat only uses either natural gas or propane, etc. From a commercial perspective, the requirements of the economics of scaled production and distribution disfavors variables. In fact, in the energy sector the comparative lack of scaled production can even be said to contribute to the delay of development of alternative energy sources. From an individual perspective, depersonalization and limited choice often accompanies scale. There are trade-offs for individuals joining networks, and in the emerging world of data networks, there is increasing pressure on service providers

to educate their users regarding those trade-offs, as they are in the best position to do so. Future IoT data rights management self-regulatory structures will be most sustainable where they include mechanisms (such as relevant metrics and feedback pathways) so that all impacted stakeholders can develop realistic expectations regarding data usage that are accountably met, minimizing the subjective sense of inconvenience.

d. Individual efficacy

IoT provides individuals with the opportunities to "think globally and act locally" in ways never before imagined, with implications for individual efficacy, governance, and innovation policy, as well as for new IoT marketing strategies and adoption models. When thermostat users are able to measurably associate their energy usage choices with global resource and climate challenges, personal efficacy grows.

i. Traditional Thermostats

Efficacy is defined as the ability to achieve a desired result. "Efficacy" is a narrow concept in the context of traditional thermostats, since although they provided the efficacy of temperature control to individuals, the ability to produce that desired result is of utility to individuals only in that local context of a single HVAC system.

ii. Data-Enhanced Thermostats

As noted above, remote control of HVAC systems increased personal efficacy, albeit still only with respect to the operation of the subject HVAC system.

iii. Networked Thermostats

Networked data systems build individual efficacy. IoT enables users to gain the perspective of expanded data access to make better decisions. Those decisions may involve issues such as system purchase and operation options, conservation strategies, and the timing of fuel purchases. An informed consumer can also act more effectively to achieve their goals and increase their efficacy as an energy supply chain participant, improving resource conservation efforts more broadly.

IoT allows individual users to enjoy the leverage of large institutional operators. Networked data transfers are mediated interactions. Once users are helped to understand the terms of data-related mediation risks, efficacy can be pursued by making smart system participation choices with attention to the best entity to perform that mediation on their behalf. A user will be best served by associating with a powerful institution with which their interests align, that can protect their interests when data about the user is made available to third parties. An informed consumer is the best IoT customer.

IoT enables communities of interest to assemble around common interactions creating individual ties to new communities, enhancing individual efficacy. Just as there are communities of fitbit™ users who compare exercise statistics, one can readily imagine communities of smart thermostat users interested in comparing energy-related data. Those COIs could organize themselves to promote the interests

of members, and could use real-time data from systems to help individuals verify things like incentive eligibility and other individual benefits derived from IoT deployments of interest to members of each such COI.

e. Greater self-knowledge

i. Traditional Thermostats

Traditional thermostats freed up individuals to pursue activities other than those associated with ambient temperature regulation, but they are not usually considered vehicles for the acquisition of individual self-knowledge.

ii. Data-Enhanced Thermostats

As noted above, HVAC systems with remote (whether or not third party monitored) access capabilities offer greater convenience to users and greater security and perhaps efficacy, but not any measure of self-knowledge.

iii. Networked Thermostats

IoT enables individuals to gain fine-grained insight into their behaviors, and to compare them with other individuals, enhancing self-knowledge.

Energy is delivered through massive networked systems. Nearly every consumer of energy, including for home heating, is connected to these systems. The behavior of populations of people establishes the performance criteria for these systems, but the individual consumer cannot usually measure their role (except with respect to the price paid for energy). Conservation and various consumption "best practices" have long been recognized as critical components of ecological approaches to energy, but the metrics have not been available to provide individuals with feedback on their impact, particularly in "real time" to affect their decision-making. Some local community energy providers have launched programs through which people are informed about their energy use relative to their neighbors. With IoT, comparisons can be made at larger scales offering greater potential insight at multiple scales.

For me to have access to that comparative energy-use information, others must be willing to provide data about energy use. Similarly, for others to be able to improve their energy consumption habits, I must be willing to provide some data about my habits. We are both benefited by the insights for which we both must take on a disclosure obligation. This setting invokes the concept of "mutual altruism," a sort of "empathetic selfishness" alluded to earlier in this white paper. Since we all seek data to inform our actions, you and I (and the institutions that act on our behalf) are other people's privacy problem, and they (and their institutions) are the source of ours. It is this embrace of this co-dependency that is the basis for future data rights governance systems.

The comparisons enabled by IoT create differences in kind, not just degree, in the insights available to individuals about their roles in groups. This is because comparative performance metrics are fundamentally different (ordinal numbers)

than single-system performance metrics (cardinal numbers). If you know how much heating fuel you use, that doesn't tell you anything about how much fuel efficiency performance your system achieves versus others, so it cannot inform you as to whether you could save money by switching consumption strategy. Access to other system data is needed to make such comparisons, and that is only available if users agree to "pool" their data for mutual benefit, knowing that they are among the beneficiaries. Various strategies are available to temper the potentially intrusive effects of such pooling (such as "zero knowledge proof" strategies). IoT enables the generation of ordinal metrics to facilitate comparisons from which users can enhance their self-knowledge.

f. Value realization

i. Traditional Thermostats

Traditional thermostats provide the benefits described above, but do not also generate additional, separate value for their users.

ii. Data-Enhanced Thermostats

Data-enhanced HVAC created new benefits for users as noted in this paper, but do not generate separate new value for users.

iii. Networked Thermostats

IoT offers new sources of value to individuals since it introduces an entirely new and separable set of interactions from which value can be created. These include (i) the value of leverage of data collected from IoT users (enhanced data output value), and (ii) the value of enhanced information seeking capability for individuals (enhanced data input value).

(i) Data leverage value. Data is the "feedstock" of valuable information that makes a difference in people's lives. While it increases the risk of privacy-type intrusions, the multiple uses of a single datum to inform multiple parties reflects the enhancement of value through data leverage. The "consumption" of data is also the "production" of valuable information in a context. Greater consumption of data yields more overall information value.

Consider that a IoT provider collecting data about thermostat settings might make that data available to both the homeowner and (with permission) also to sellers of insulation for advertising (1x leverage), sellers of wool socks for advertising (2x leverage), and local energy utility for load shaping (3x (non-monetization) leverage). The one item of data can be leveraged to three (or more) items of information, limited only by the number of parties interested in that data (and by any contrary rights of the data subject and other parties in the "data-to-information supply chain"). In a sustainably structured system, a portion of the new value created through leverage is applied to offer incentives to data subjects to encourage their participation. This structure is applied in myriad free online services that are paid for by advertising. Systems that leverage data mostly for advertising to date (even though generating vast wealth) have just taken initial data leveraging steps; in

fact the monetization of data through advertising on the Internet is really just a minor modification of the business strategy of networked television in the 1960's. Advertising is just a small subset of how data is used by humans, suggesting that additional leverage opportunities abound.

Future systems will likely explore data leverage beyond advertising, and may also explore additional and alternative incentives funded by value produced from data feedstock beyond merely providing "free" online services (the primary function of which is to attract users that produce data). Some of those alternative value propositions may initially find traction in the IoT, which tends to have a lower interaction rates and less detailed UIs than online services such as social networks.

(ii) Information seeking value. Every day we seek high quality information on which we can rely. That information has value to us. Much of that information involves the current behavior of others, and its accuracy is dependent on participation rates. For example, traffic reports are not useful if we only know about 50% of the cars, and predictions of energy use are not useful if they only include 50% of houses. Data value is predicated on data quality, which is improved as participation levels increase. Future IoT systems and their users will benefit from the use of incentive structures that foster participation through reliability to improve the quality of data sets, for the mutual benefit of the information-seeking activity of their participants.

g. Individual security

i. Traditional Thermostats

Traditional thermostat systems provided a form of "thermal security" by reliably maintaining temperatures within user-defined parameters. This was not just a matter of comfort and convenience (as discussed above), since temperature stability also had economic implications even in early thermostat deployments such as poultry incubators and textile mills.

Traditional thermostat systems also offered data security given that they were non-networked, and the data generated by the system, taken alone, was generally insufficient to raise security concerns if it was subject to unauthorized access.

ii. Data-Enhanced Thermostats

With data-enhanced HVAC, off-site third party monitoring was enabled. This meant that HVAC users could pay someone to monitor their system operation data, increasing (or at least "outsourcing") reliability of security associated with heating and cooling.

Where third parties are retained to help an individual with their "information seeking" behavior of home monitoring, some risks are mitigated and new risks arise. When third parties become involved in providing individual benefits, the concept of "trust" also becomes relevant. For non-networked deployments of third party services, subjective reputation information (such as friend's recommendations)

helps to inform the choice of trusted service providers. However, for distributed and networked deployments, objectively testable standard performance metrics are more scalable and helpful.

iii. Networked Thermostats

Traditional thermostats secure the local physical environment against risks of temperature change. IoT signals the constitution of non-physical "information environments" with new benefits, and new risks. The thermostat initiates system action based on feedback between the environment and user preferences. What is the nature of the feedback that is needed to support user preferences in information environments? The feedback that measures user preferences will be focused on whether the system reliably delivers on promises of user benefits. Thus, whatever the specific "metric" of a given feedback loop, what are sought by users is indicia of "reliability."

In fact, reliability of system operation can be argued to be foundational to achieving both security and privacy in IoT; challenges to both of which can be said to represent the absence of reliability. Reliability is boring, which is a desirable characteristic of networked systems on which we rely – reliable systems fade into the background. Exciting electricity is a blackout. Exciting water service is a flooded basement – we notice these services when they become unreliable and risky, compromising our security. Data "services" are exciting at present, so much so that they are not yet sufficiently boring to be considered reliable. Part of the challenge is that stakeholders have not yet identified ways to measure data service reliability to discern if they are "boring" or "exciting." Security will increase when data systems are made measurably boring – like a thermostat.

Security is changing as physical risks morph into information risks. Importantly, the ubiquity of existing deployment of mobile devices already bristling with sensors may help to moot many of the data security concerns associated with thermostat and other home IoT deployments. This is because people carry their mobile devices into their homes at the end of the day, and with them a huge number of sensors (including those that detect temperature, humidity, light, acceleration, position and other physical qualities). IoT is less alarming to the extent that IoT data is duplicative of that already generated by mobile devices while present in the home.

Security can also be enhanced by IoT. Fortunately, the source of the challenges is also a source of new solutions. For example, networked HVAC data in IoT can be combined with other home sensor data (such as fire alarm and burglar alarm data) to enhance overall home security awareness for individual homeowners.

Paradoxically distributed systems offer anonymity to criminals, but they also enable new distributed security strategies. When data about an individual is embedded in sets of data about others and is fed back to them, it enables the individual to make comparisons. Among the possible comparisons are whether one of more of the observed systems is operating outside of conformance with system parameters.

Relative performance of systems can reveal to users evidence of accidental or intentional misconduct in meta-system function. In essence, IoT gives systems "1000 eyes," enabling stakeholders in a given trust framework to create a "neighborhood watch" for their community of interest. This heightens overall security, and in fact may become an ascendant paradigm for security deployment in distributed systems at all scales, particularly where centralized security hierarchies have demonstrated decreasing efficacy. It is not unlike the security value added to a gas distribution system when a neighbor smelling gas in a neighborhood calls the gas company. In fact, gas companies add Mercaptan to otherwise odorless natural gas as a security measure to "recruit" the noses into being biological sensors, their "gain" set to high by mutual altruism in the community of interest of a physical neighborhood. No one wants a gas explosion, so everyone is tuned in to the smell of gas. One whiff of Mercaptan and everyone is on "orange alert."

Finally, IoT can also be viewed as a form of information "outsourcing" available to individuals. Outsourcing has many security-related benefits for companies, many of which will also be of interest to individuals. This includes the ability to seek expert help for a particular issue, the ability to leverage services in third party networks, and the ability to secure contractual assurances regarding identified risks. As is the case with commercial outsourcing, individuals will derive security (and related privacy) benefits from the reliability of established providers of IoT services, who are best able to deliver on their promises. It will be important that data subjects fully understand those promises (typically made in terms of service and privacy policies), and are able to rely on them.

III. The Privacy Concern

Privacy is a hot topic in IoT products such as smart thermostats. What was once a simple device for maintaining a comfortable environment in the home has now been swept up in the networked information revolution. The new individual benefits and new privacy risks both seem potentially unbounded, primarily because we don't have any established ways to measure either.

The Internet of Things (IoT) is an artifact of Moore's law, and is a concept that is meant to anticipate the emerging setting where the many devices and objects with which we interact can cost-effectively be given a sensory capacity and/or a data transfer capacity to capture and transmit (and sometimes process) data about their environment and their operation in it. Where that environment includes humans, a portion of collected data will be "about" that human activity, providing new insights and raising new privacy concerns.

As a result, the once unknown details of interactions of people and things can now be collected, transferred and processed at trivial cost. This vastly increases the data flows regarding such interactions (such as with a thermostat), which can inform users, suppliers and others about performance and other aspects of such interactions, yielding greater insight into such use.

Where that insight has the potential to harm the interests of an individual or entity it is viewed as an "intrusion." In fact, insight and intrusion are two opposing perspectives on the single phenomenon of the creation of infor-mation that occurs when data "informs" a given party in a context. Effective metrics for shared management of privacy controls will allow multiple stakeholders to simultaneously weigh various forms of insight and intrusion to inform their participation decisions. The aggregate of those decisions will give rise to new interaction governance structures as candidates form emerging data rights institutions.

The march of IoT and the irresistible information potential of valuable "big data" is in the process of making data a commodity asset, anticipating its broad use and trading. This raises a number of challenges, including how best to preserve and enhance individual rights in those settings where a particular re-combination of stored data yields information that relates to a person, the use of which is perceived as a potential invasion of privacy and other individual rights. New insights and new intrusions are enabled by new combinations of previously isolated types of data that cannot be anticipated at the time of data collection (narrowing the effectiveness of traditional "notice and consent" conversations at the time of initial data collection). To address this dynamic risk, it seems that the paradigm of privacy protection will need to shift from relying chiefly on limitations on the single event of "data collection" to increasingly focusing on limitations applied serially at the times of multiple "data use," particularly given the ever increasing torrent of data that is available ever more inexpensively in the data deluge of IoT.

"Use" limitations are typically preferred to "efficacy constraint" as a strategy to deal with the harmful uses of powerful technologies. Data is a "dual use" technology that lends itself more readily to "use" regulation, particularly if "big data" is to reach its potential. This paper will examine the issue of privacy through the same three lenses of benefit applied in section II above: traditional, data-enhanced, and networked thermostats.

i. Traditional Thermostats

Traditional thermostats were "private" in the sense that data relating to their operation was not made directly available to others, but privacy was never really a consideration for how one set their thermostat. There was little or no perception that awareness of another's thermostat settings might be intrusive.

Some third-party data collection is, in fact, already a feature of residential HVAC. Home heating habits are recorded in the billing history of a residential heating customer that reveals their consumption patterns and the price they paid for energy at a level of detail that is dependent on the metering and billing cycle. . In the U.S., usage data is collected by energy distributors and can be made available to participants in energy markets. Parties in energy supply chains can combine this data with other data for planning, marketing, load balancing and a host of other purposes.

Notably, under traditional 4th amendment jurisprudence (which, in the absence of other standards, is frequently invoked in U.S. privacy contexts), billing records, such as for home energy use, could be considered "business records",[3] so that the data they contained would not be deemed to be "reasonably expected" to be kept private by the company engaged in the billing. Since the company has already "seen" the billing data, the customer is considered to already "know" that it is not private, precluding constitutional protection under the "reasonable expectation" test. This exception from protection against unreasonable "search and seizure" could relieve a governmental investigator of warrant and similar requirements when seeking access to such billing data for evidentiary purposes.

IoT in thermostats and elsewhere in the home has the potential to increase the granularity of such "business records" data, raising its potential for insight, and its availability, raising the potential for intrusion, into the lives of individuals, with implications for constitutional and statutory individual rights. In societies that seek to maintain a sustainable balance of privacy and sanctioned investigatory interests, it is conceivable that IoT will prompt a reexamination of the nature of the "reasonable expectation" test, particularly as it is referenced in contexts beyond criminal proceedings.

[3] See, e.g., U.S. v. Miller, 425 U.S. 435 (1976) and Smith v. Maryland, 442 U.S. 735 (1979).

The absence of 4th amendment protection against intrusion into such business records invites consideration of alternative regimes for their protection, particularly in the context of commercial uses of data. The non-governmental use context, and the reality of global deployment of information networks, suggests that future privacy protections of such data will depend upon sources of authority beyond that of individual jurisdictions. Outside the realm of government action to seize evidence that is addressed by the 4th amendment, the issue of privacy can be dealt with contractually in the Terms of Service of the service provider(s) that collect and use the collected data. In that broader context where rights are mapped by contract, the constitutional exception that applies to open up business records data to public safety authorities can be narrowed to provide individuals with greater privacy protection against private intrusions into the contents of business records. Such contract rights won't affect 4th amendment analysis, but can offer enforceable, enhanced privacy benefits to individuals in every other context.

ii. Data-Enhanced Thermostats

Earlier data enhanced HVAC was typically provided by a single supplier, which limited the scope of potential data transfer, enabling its treatment to be addressed as part of the service agreement.

iii. Networked Thermostats

In the past two decades, technology advances have caused our information environments to become richer, as higher connection speeds and technologies have lowered prices, enabling the placement of sensor and data transmission technologies at increasingly small scales. We all benefit from these advances, and all have had to adjust to the costs and implications of being increasingly monitored and observed as adoption roars ahead. This setting feels less private, and it is, based on an expectation of privacy derived from a different time, and a different point in the history of ICT.

Privacy was easier when data wasn't connected. The default setting of all data systems was maximum privacy when physical data isolation yielded *de facto* secrecy. Data secrecy was an artifact of pre-networked systems. The secrecy intrusions ushered in by prior networked technologies (such as postal, telegraph and telephone systems) were dealt with by combinations of secrecy-enhancing technologies and laws within jurisdictions, a strategy that is strained in the global Internet context. It is possible that data secrecy is dead or dying with enhanced global networked information interoperability, accelerated by IoT, but privacy doesn't have to die with it. The Internet of Things will challenge our current notions of secrecy and invite us to employ more affirmative measures to enable the provision of privacy (not just as an accident of secrecy), and it will also invite us to act with more intention to understand how our actions affect others and future generations (and ourselves through "mutual altruism"). Conceptions of privacy tactics such as data collection limitation and the "right to be forgotten" reflect an understandable nostalgia for a time when privacy was an artifact of constraints of accidental secrecy. That time is past.

As technology (and in particular networked information technologies) have whittled away at secrecy, we have seen privacy and security diminish. This is a result of our continued reliance on approaches to privacy and security that were developed when there was more secrecy. Our risks have changed, but not our risk mitigation strategies. Faced with rapid change, we look to our old institutions for risk mitigation answers, but the institutions stand mute, completely unable to self-adjust their respective programming to adjust to the new risk circumstances.

Fortunately, the source of the problem is also the source of the solution. IoT has the capacity to enhance real privacy based on its provision of more specific and fine-grained measurement that can be applied to assure the accountability of data handlers and enforceable rights of data subjects, which will supersede the haphazard forms of privacy that were derived from functional artifacts of the "secrecy" that was itself an artifact of now-anachronistic forms of ICT technology. In short, with the death of secrecy, privacy will be most effectively achieved as a "social good" based in measurable mutual respect for rights manifested in enforceable duties to create boundaries of data usage in various identified contexts.

In fact, once the various traditional and emerging privacy rights are described in terms of specific duties to protect individual data "input" and "output" actions (i.e., expressive and perceptual information channels) in a given system (based on cultural norms, group expectations, etc.), privacy becomes an operational problem, akin to security, in networked information systems. It is possible to conceive of a reliable data collection, storage, transfer and processing operations layer that could provide data-related services to different data parties in different COIs, including individuals enjoying enhanced privacy benefits.

The paradox of "big data" with "privacy" (and "security") can be resolved if stakeholders are provided with shared metrics for evaluating data channel (input and output) integrity. That will provide a measure of "privacy" (and security) that can be dynamically tuned to the context and the subjective preference of the data subject (and their respective COIs), in a manner that more closely resembles familiar privacy choices currently dynamically available to individuals in physical space.

When privacy and security are defined as emerging from channel integrity issues, attention turns to how such channel integrity can best be achieved. Larger data and Telco operators are likely to provide more stable and reliable data channel integrity to stakeholders, since they have the greatest resources and experience in preventing third-party intrusions, and their business plans, brand reputation and shareholder value depend upon their being trusted by large populations of users. Once IoT data, such as HVAC data, enters the network, it can be most reliably handled and accounted for by a large data operator, as opposed to a local heating company for example.

In privacy, one size does not fit all. When "privacy" is viewed as involving identity channel (input and output) integrity, it becomes possible to easily and measurably adjust the degree of such input and output channel integrity to suit individual needs, and to "mass customize" the privacy experience of individuals and companies. Such adjustments might resemble, for instance, the variations described in U.S. NIST 800-63[4] associated with different identity "levels of assurance" which acknowledge that different levels of "channel integrity" in the flows of identity data channels are appropriate in different risk contexts. This "tunable" approach to channel integrity anticipates the emergence of "privacy as a service," which relegates to the past the notion of "privacy as an artifact (of secrecy)" (which died with the distributed internet) and instead, embraces a more scalable version of privacy as an emergent aspect of reliable services offered to individuals in networks.

With IoT, the data production floor is literally at your fingertips, and the distribution channels are non-local. Privacy was once a "local" problem solved by closing the shades. As it has become a non-local problem with distributed networked data systems, strategies of maintaining privacy must shift from resource intensive attempts to artificially preserve secrecy in a distributed domain (which is ultimately futile given the opposing "power law" problem of network expansion) to those that move beyond secrecy to answer the question: What do "privacy" and "security" mean now that data is non-local? This is not a call to fully abandon efforts to "obscure" local instances of data in an effort to replicate the secrecy of the past, but rather an observation that exclusive reliance upon such "artificial secrecy" will ultimately yield to the overall information seeking behavior of systems as they manifest matured forms of systemic artificial intelligence, as many data markets already do. Privacy strategies based on local, centralized protection have been undermined by technological change, as has the authority of institutions that promulgate exclusive reliance on those strategies. New strategies that recruit affected stakeholders to be part of the solution can scale, empowering participants, and their standardized rules and technology tools will give rise to new, additional institutional structures that are "fit for purpose" in providing privacy at Internet scale.

[4] See, e.g., NIST Special Publication 800-63-2, Electronic Authentication Guideline (August, 2013).

IV. Conclusion

The conclusion of this white paper is that the IoT will accelerate the deployment of "big data," but that attention to individual benefits (including the assurance of privacy and security) in IoT design, development and deployment is a key to assuring that the default settings of "big data" are favorable to individuals, and that IoT systems are sustainable economically, socially and culturally. In the absence of these considerations, there is a substantial likelihood that the economic and engineering focus on efficiency, as a super-factor will drive the default architecture; a result that will not foster all individual goals and will institutionalize tensions with users that will undermine sustainable system function. Sociotechnical systems require sociotechnical (as opposed to purely technical) architectural solutions.

The IoT has been rendered inevitable as the result of a confluence of historical trends, but the choices that we make now regarding its fundamental architecture that can tip the balance of harm and benefit of IoT more toward either individual or institutional rights and obligations. The choice is ours (collectively) and the time is now.

Relevant shared metrics across networks are the key to getting the balance right; since those shared metrics enable "cross-talk" across stakeholder perspectives. Money is an historical example of a shared metric that crosses domains, albeit one that is limited to the measurement of the subset of monetize-able benefits. Expanded sets of metrics can be derived from a mapping of benefits and burdens across stakeholder groups in networked ICT (and stakeholders in sectors served by ICT – such as those humans affected by "climate change" in the case of smart thermostats). Some of those metrics might even find application in various initiatives to supplement measures of sustainable growth beyond traditional GNP-based macroeconomics. In an effort to empower individuals to embrace the distributed strategy to "think globally and act locally, it is helpful to apply the tactics based on "what gets measured gets done."

The metrics can help to discern the presence (or potential presence) of benefits to individuals and groups. System designers considering technological and policy choices for future ICT systems are already working to incorporate performance standards based on various metrics that relate to historically identified harms and benefits. Metrics relating to emerging individual benefits and harms should be among them to help drive adoption, and to anticipate future individual needs. In fast moving IoT, the authority of the past needs to be supplemented by the authority of the anticipation of future needs of stakeholders. Individuals, service providers, data users, and future auditors, assessors and self-assessors of system requirements will apply these metrics in future evaluations of system performance.

Once the architectural choices that reflect these balances are "baked in" to default settings of technology and policy deployments that are broadly deployed, they will

function like a rights "block chain" (to borrow from the current parlance), and be more difficult (albeit not impossible) to alter in future IoT iterations. The precedent of human habits functions as a behavioral-rules block chain that can form a core of trust for the human part of socio-technical systems from which sustainable, reliable and scalable systems of leverage and risk reduction can be deployed at large scales. The identification of individual benefits is also first step toward developing performance standards that can manifest such benefits; with relevant metrics providing a sense of performance against such standards for all stakeholders to convene broader participation and a cyclic process of benefit innovation for individuals and institutions.