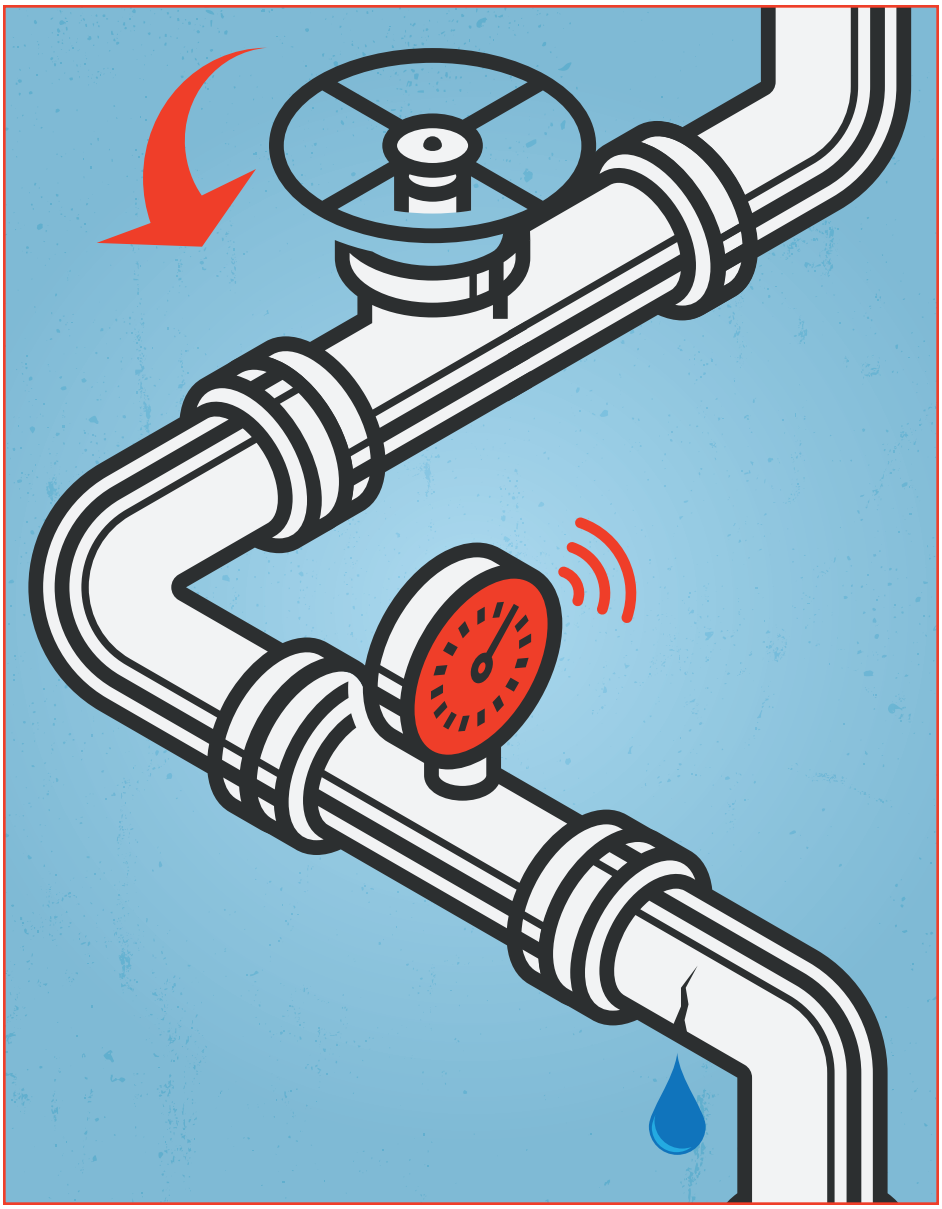
Summer 2018 Volume 15, Number 2

# iHOMES and BUILDINGS

THE MAGAZINE OF THE CONTINENTAL AUTOMATED BUILDINGS ASSOCIATION



How Automation Solutions are Solving one of the Biggest Risks for Buildings

Privacy in an IoT World

Artificial Intelligence and the IoT Connected Home

Building Connectivity and the Cost of Disruption

Where Is Wi-Fi Heading?

Integrating Energy and Facility Management

CABA™ Connect to what's next™

www.caba.org/ihomesandbuildings

# iHOMES and BUILDINGS

THE MAGAZINE OF THE CONTINENTAL AUTOMATED BUILDINGS ASSOCIATION

Summer 2018, Volume 15, Number 2


## Contents


**Features**

Large Building Automation

How Automation Solutions are Solving one of the Biggest Risks for Buildings by Nadine Evans ..... 7

Home Systems

Where Is Wi-Fi Heading? by Cees Links ..... 13

**Columns**

CABA President & CEO's Message ..... 3

CABA Research Briefs

Integrating Energy and Facility Management ..... 5

10 Hot Consumer Trends 2018 ..... 6

Ken Wacks' Perspectives

Privacy in an IoT World ..... 9

Research Viewpoints

Artificial Intelligence and the IoT Connected Home by L. Anne Breene & Lawrence Silverman ..... 11

Opinion

Building Connectivity and the Cost of Disruption by James Carlini ..... 19

**Departments**

New Members ..... 4

Upcoming Events ..... 21

# iHOMES and BUILDINGS

THE MAGAZINE OF THE CONTINENTAL AUTOMATED BUILDINGS ASSOCIATION

Summer 2018
Volume 15, Number 2





CABA™ Connect to what's next™

**Association Office**
Continental Automated Buildings Association
1173 Cyrville Road, Suite 210
Ottawa, Ontario, Canada
K1J 7S6

Tel: 613.686.1814; 888.798.CABA (2222) Fax: 613.744.7833





For subscriptions, circulation, and change of address enquiries email caba@caba.org. For editorial and advertising opportunities: www.caba.org/ihomesandbuildings

# Ken Wacks' Perspectives

## Privacy in an IoT World

By Ken Wacks

There is an enduring myth that "my home is my castle." I can close the door against unwanted intruders. The founders of the United States enshrined this in the fourth amendment to the U.S. Constitution limiting government power to search a person's home. However, this does not apply to private companies.

In this paper, I examine the reality, benefits, challenges, and possible technical solutions for excessive collection of private customer data. Technology is emerging in the form of communication gateways and premises equipment specifically programmed to guard and limit access to private data.

I chair the international committee responsible for standards to facilitate connected devices in homes and small buildings. At our March 2018, meeting we focused on enhancing gateway standards to protect consumer privacy, safety, and cyber security. I will explain the privacy challenges in this article and our methods for enabling privacy protection via enhancing the gateway technology in the next issue of *iHomes and Buildings*.

### Data from the connected home

The world of IoT (Internet of Things) is a connected world of home devices and external servers, which may be owned and managed by the device developers. Smart thermostats communicate with the vendor's server as part of a learning program to improve comfort; smart TVs communicate with the manufacturer for app functions including voice commands. The relationship among services and home devices is illustrated in Figure 1.

Consumers make tradeoffs about providing personal data in exchange for services. For example, we may provide credit card details for a purchase. Sometimes we divulge personal preferences in order to purchase custom-designed products, such as clothes or entertainment. We might assume that such personal data use will be limited to providing specific products or services. Services that involve connecting to external servers pose a challenge. Smart devices using these services can easily track daily activities of the occupants and maintain a record in the servers.

The reality is that data are becoming valuable as a resource to be mined for targeted advertising. Advertisers like targeted ads because they reach more likely potential customers than traditional broadcast advertising where everyone gets the same ads. In some cases, law-enforcement personnel are mining such data without a search warrant on the basis that the information was voluntarily released, even if you did not know the data were being collected.

Even when an ethical service provider promises to protect customer data without selling or sharing the data, there is usually fine print in the "click-through" service agreement that acts as an escape clause. Privacy agreements caution customers that the terms may be changed. Data protection promises might be gone if the company is sold. The U.S. government is now allowing Internet Service Providers to mine customer data and use these data for any purpose without notifying the customer.

### What is privacy?

The U.S. National Institute of Technology and Standards (NIST) wrote a 600-page three-volume interagency report on *Guidelines for Smart Grid Cybersecurity*[1]. I contributed to Volume 2, *Privacy and the Smart Grid*. We debated the meaning of privacy and concluded [quoted from Section 5.2 of Volume 2]:

> There is not one universal, internationally accepted definition of "privacy"; it can mean many things to different individuals. At its most basic, privacy can be seen as the right to be left alone. Privacy is not a plainly delineated concept and is not simply the specifications provided within laws and regulations. Furthermore, privacy should not be confused, as it often is, with being the same as confidentiality; and personal information is not

1. NISTIR 7628 Rev. 1, *Guidelines for Smart Grid Cybersecurity*, September 2014. Available free at https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final

the same as confidential information. Confidential information is information for which access should be limited to only those with a business need to know and that could result in compromise to a system, data, application, or other business function if inappropriately shared.

Additionally, privacy can often be confused with security. Although there may be significant overlap between the two, they are also distinct concepts. There can be security without having privacy, but there cannot be privacy without security; it is one of the elements of privacy. Security involves ensuring the confidentiality, integrity, and availability of data. However, privacy goes beyond having proper authentication and similar security protections. It also addresses such needs as ensuring data is only used for the purpose for which it was collected and properly disposing of that data once it is no longer needed to fulfill that purpose.

We categorized privacy into four dimensions [quoted from Section 5.2]:

1. **Privacy of personal information**. This is the most commonly thought-of dimension. Personal information is any information relating to an individual, who can be identified, directly or indirectly, by that information and in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, locational or social identity. Privacy of personal information involves the right to control when, where, how, to whom, and to what extent an individual shares their own personal information, as well as the right to access personal information given to others, to correct it, and to ensure it is safeguarded and disposed of appropriately.
2. **Privacy of the person**. This is the right to control the integrity of one's own body. It covers such things as physical requirements, health problems, and required medical devices.
3. **Privacy of personal behavior**. This is the right of individuals to keep any knowledge of their activities, and their choices, from being shared with others.

Table 1: Privacy Policy Issues

| Privacy topic | Customer options |
|---|---|
| Data collected | What data are collected?<br>When and how often are data collected?<br>Can the customer update the data? |
| Services provided | What services will be delivered in exchange for providing these data?<br>Are there options for reduced services requiring less personal data?<br>Will these data be used for purposes other than providing specific services? |
| Data access and accuracy | Who has access to these data?<br>How can the customer review the data for accuracy?<br>How can the customer correct or revise the data?<br>Will these data be transmitted or sold to third parties?<br>Will these data be correlated with other databases for "data mining"?<br>Will these data be aggregated? If so, will personal details be removed? |
| Data deletion | How long will collected data be retained?<br>Will data be archived or erased after the retention date?<br>When will backup files containing data after the retention date be purged?<br>Will the customer be notified when the data and backup files have been erased? |
| Privacy policy changes | Is the consumer notified of any changes in the privacy policy?<br>What options are available to the consumer if the privacy policy is changed? |

**Practical Connectivity with Data Security in Homes and Buildings**
Toronto, Ontario, Canada – March 23, 2018

The promise of seamless connectivity while protecting consumer privacy, security, and safety when using Internet of Things (IoT) in homes and buildings is nearly here. The world standards body responsible for publishing technical standards enabling business and trade through information technology (IT) is developing a family of standards that interconnects disparate networks and products to deliver unified customer services. These standards allow consumers to mix products and services from various manufacturers in order to create a personalized environment where everything works. Lighting, entertainment equipment, heating and cooling, health and safety systems, solar power, electric vehicles, and appliances can be coordinated to adapt to the and deliver services automatically like an electronic butler. The data traffic among this equipment is continuously monitored to ensure that customer privacy and safety are protected with cyber security sentries monitoring data flows.

Consumer electronics and IT experts from Asia, Europe, and North America gathered this week at Eaton Corporation in Toronto to continue work on a series of standards under ISO and IEC for home and building automation systems. This group so far has produced 50 standards for the Home Electronic System (HES) that includes communication protocols, network management, and applications for automation in homes, apartments, and small commercial buildings. These standards offer manufacturers an infrastructure for creating unique and exciting products to enhance living and working in homes and buildings. By developing products based on a standard infrastructure, manufacturers can focus their expertise on applications that deliver novel customer experiences through innovative products.

Gateways link home and building networks with outside networks such as the Internet. HES extends the conventional gateway with support for multiple home and building networks. The HES gateway translates and relays messages among these networks. The gateway also determines if messages should be exchanged with outside service providers. Messages may be blocked if they convey unauthorized private data or could initiate an unsafe action such as turning on an unattended, potentially dangerous appliance.

The HES standards are specifications for products that allow customers to manage the dissemination of their personal data. Agreements between vendors and customers can be negotiated according to competitive situations and local practices. The HES gateway enforces contracts between customers and service providers to ensure that only authorized data are sent. Empowering customers with HES technology that offers options for flexible data management should alleviate customer concerns, thereby facilitating the growth of IoT markets involving homes and buildings with links to cloud and smart-city services.

**About HES**
Home Electronic System (HES) is being produced by the international standards working group, ISO/IEC JTC 1/SC 25/WG 1 , which develops standards for the interconnection of electrical and electronic equipment and products for homes and small buildings. The primary markets for WG 1 standards are designers, manufacturers, and installers of these products and related services.

**Contact**
Dr. Kenneth Wacks
HES chair
www.kenwacks.com
781.662.6211
kenn@alum.mit.edu

4. **Privacy of personal communications**. This is the right to communicate without undue surveillance, monitoring, or censorship.

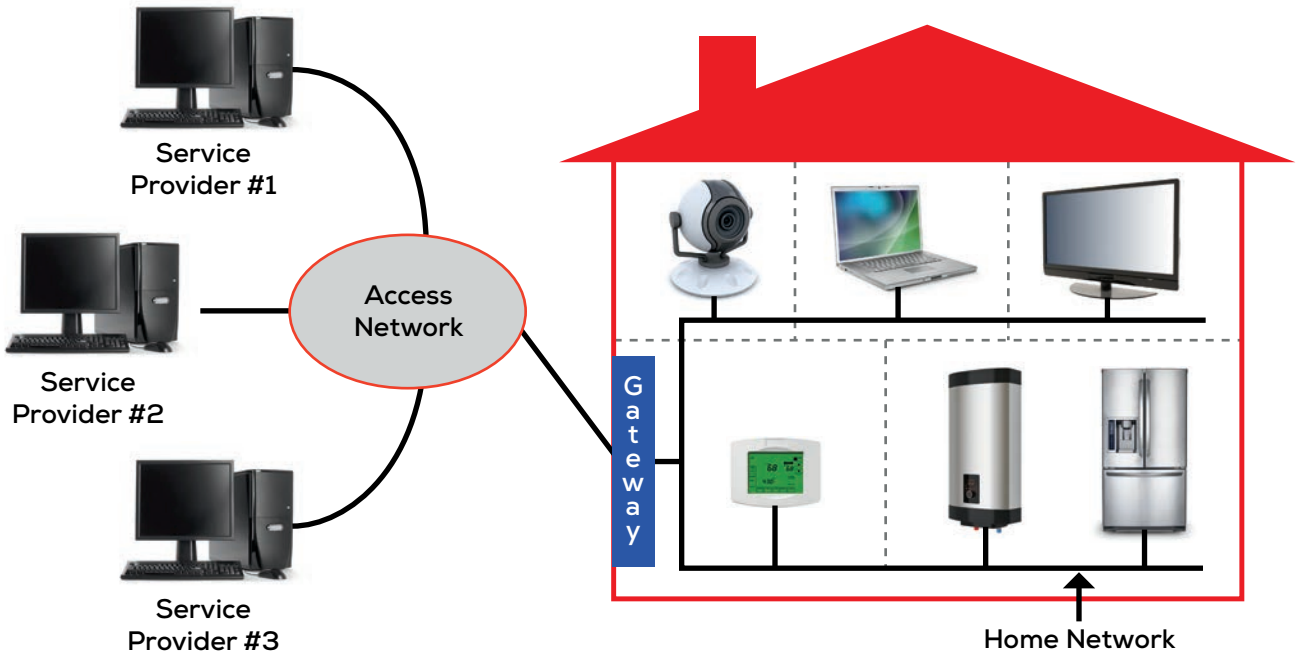
## Use of customer data

We are entering an era of what I call "data vacuuming," where all data sent by IoT devices to servers will be retained for future monetization. Even organizations such as public utilities that are precluded by regulation from data mining are collecting data with the expectation that regulations may be changed. Monetizing such data could extend beyond ads tailored to the home occupant by creating a customer profile useful for insurers, employers, politicians, and the government.

Imagine a world where you pay higher auto insurance because you have enjoyed reading about race cars or demolition derbies on the Internet. What can a consumer do to avoid transforming the home castle into an arena open to access by commercial and political entities?

Some vendors offer useful services that entice

Figure 1 – IoT Services Networked to Home Devices




customers. This is perfectly legitimate if the consumer judges that what is given in personal data balances what is delivered in benefits.

## Customer privacy data choices

Technology for a gateway is being specified that can help the consumer limit data collection to what was agreed or assumed in conjunction with the purchase of a service or product. With this technology privacy policies are presented as a contract between a service provider and a customer. Customers could be offered a choice of services and the corresponding personal data required. These choices are then entered into the gateway processor, which checks the data traffic for compliance with the privacy choices. To guide consumers in making informed decisions involving privacy, the privacy issues listed in Table 1 should be addressed.

## Privacy by gateway design

With most written privacy statements, there is no opportunity for negotiation. It is presented as take-it to receive the services or leave-it with no services. In my next article in *iHomes and Buildings* I will introduce new international standards under development for gateway technology options. These features enable the gateway to implement and enforce privacy. A press release previewing these standards is contained in the sidebar of this article.

We envision more options using the gateway technology to complement privacy agreements between service providers and customers when customers have choices. For example, if the privacy agreement states that certain data cannot be sent to a service provider, such as when the house was occupied and who was home, the gateway technology would enforce the contract by filtering attempts by connected devices to send such messages. Thus, the gateway becomes the home sentry providing data protection and screening for consumer privacy. The features of a home sentry will be presented in the fall 2018 issue of *iHomes and Buildings*. ●

Dr. Kenneth Wacks has been a pioneer in establishing the home systems industry. He delivers clear and practical advice to manufacturers and utilities worldwide on business opportunities, network alternatives, and product developments in home and building systems. The United States Department of Energy appointed him to the GridWise® Architecture Council to guide the electric industry toward smart grids. For further information, please contact Ken at 781.662.6211; kenn@alum.mit.edu; www.kenwacks.com.