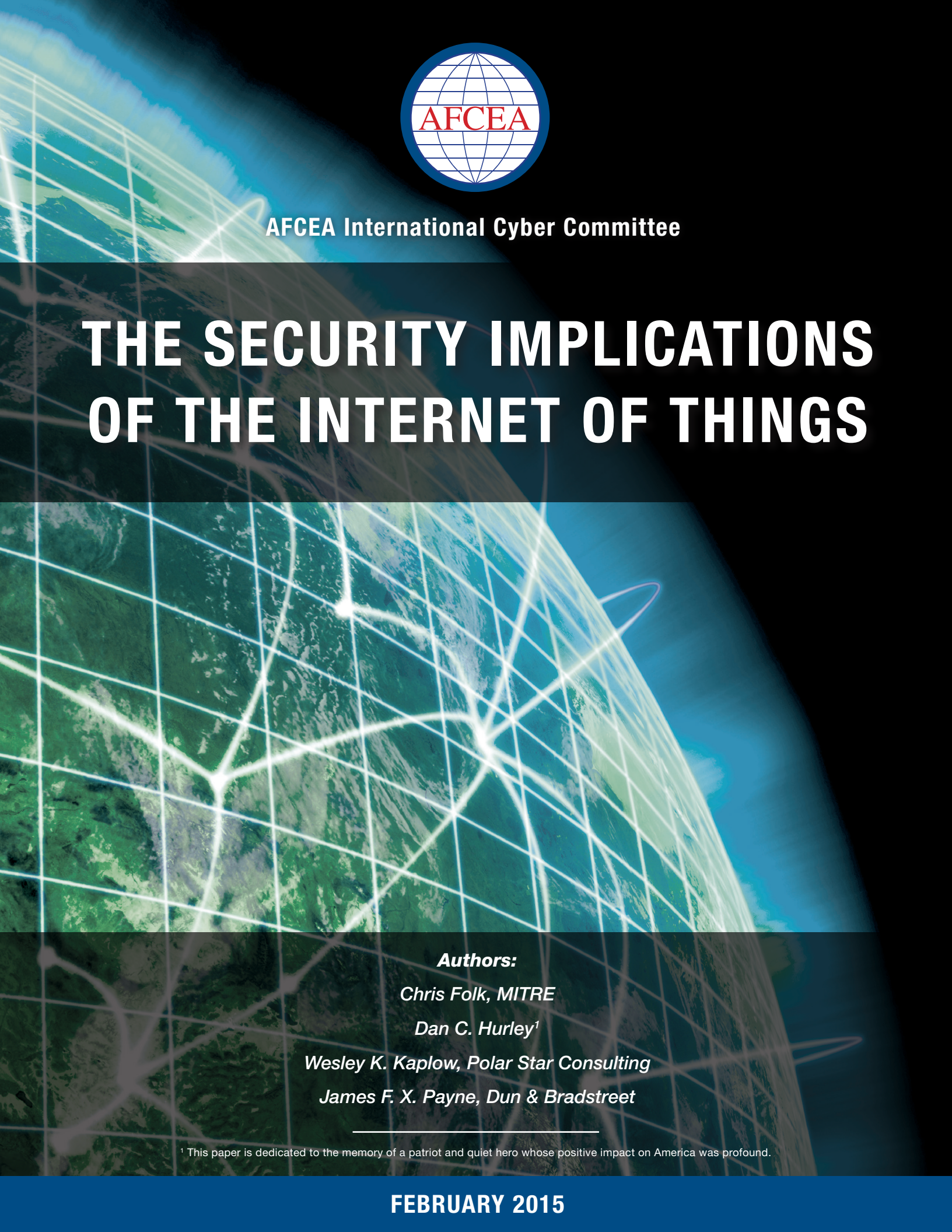


AFCEA International Cyber Committee

THE SECURITY IMPLICATIONS OF THE INTERNET OF THINGS

Authors:

Chris Folk, MITRE

Dan C. Hurley[1]

Wesley K. Kaplow, Polar Star Consulting

James F. X. Payne, Dun & Bradstreet

[1] This paper is dedicated to the memory of a patriot and quiet hero whose positive impact on America was profound.

FEBRUARY 2015

CONTENTS

TABLES AND FIGURES

Tables:

Figures:

1 EXECUTIVE SUMMARY

A vast and transformational change is happening that will alter the face of the Internet as we know it forever.[2] An explosion of connectivity under the broad descriptor of The Internet of Things (IoT) is currently rolling out across the globe, leveraging the enormous expansion of IP addresses through the carrier deployment of IPv6. This new IP protocol moves Internet addresses from a limited and carefully managed resource to a new platform without any such restriction. This dramatic change in venue has spawned a new creative spirit not unlike the first years of the Internet. This expansive change is expected to increase the number of smart connected devices by some estimates to 50 billion, or even more. With previous address restrictions lifted, creative solutions are being proffered daily that connect our healthcare, home energy consumption, mass transit, insurance, and almost every economic sector such that we will have infinitely more opportunities to optimize and simplify usage and effectiveness.

Some are calling this the Second Economy or the Industrial Internet. It is bringing upon our lives a myriad of products and services that each will have to be managed and secured. The size of this market is estimated in the trillions of dollars. It is clear from the interviews conducted in the preparation of this document that surprisingly little consideration is being paid to the cyber security of this phenomenon. In the rush to market and with very little structural regulation, goods are arriving in the marketplace without adequate preparation or explanations that will protect the consumer and society.

This wave of change is another phase of convergence reminiscent of the migration from analog to digital or private networks of the 1960s to packetized shared networks. And, like these other examples of convergence, basic assumptions about privacy and protections need to be considered now before the process, not *after* the massive rollout.

Now is the time to consider the implication of these changes and suggest means and methods of determining their impact. The purpose of this paper is to better define the threat aperture that changes with this new environment. What fundamentally makes this threat different from traditional cyber is that this involves what many call actions at a distance. Once we, as individual consumers, introduce the IoT into our families and lives, we allow machine-to-machine interactions on our behalf. This changes legal and liability issues and, in some cases, introduces a series of grey areas yet to be defined.

What do we need to consider as we race toward this new model relative to security, privacy, and long term planning at the corporate and citizen level? This white paper is a call for awareness with recommendations for actions that need to evolve just as we evolve the related technologies that enable this progress. There is a need to pause and consider the overall implication of these changes before the unintended consequences that always accompany rapid change. Nothing short of a new ecosystem may be needed.

[2] http://www.businessinsider.com/google-chief-eric-schmidt-the-internet-will-disappear-2015-1.

2 METHODOLOGY & SCOPE

Limitations of time, as well as the size of the assigned team necessitated the setting of scope. Realizing this complex problem cannot be fully resolved in such a short space, the team identified modest goals and scope. We set out to talk to industry leaders and those at the forefront of this process. We wanted to see how the thought leaders were managing and anticipating these issues and to see if we found adequate thinking and planning as these grand ideas are emerging. One of our key scoping decisions was to offer a simple list, based on these interviews, of what we thought were hot button issues that above all need to come into the broadest light for review and discussion. These are the most basic discussion points that will have potentially devastating implications if not considered. Of particular interest was the consideration of those factors that, if built into the product offering during the developmental stage, would incrementally improve basic security and prevent the many "out-boarded or bolted-on" solutions that have become standard in today's Internet. What things can be done ***before*** products reach the market to make them and services inherently more secure? What can be done economically in the planning stages, not after a disastrous event exposes a security vulnerability? This white paper ventures to offer a composite of issues that have an immediate need for attention and much further discussion and debate.

Though interviewees are identified, there is no attribution. This approach fostered candor and set a more open and forthright discussion.

3 INTERVIEWS

The team identified sources across a broad spectrum of interested parties actually dealing with the issue of security as it pertains to the Internet of Things. Over a period of three months, seven experts in the field of technology and public policy made themselves available using a variety of meeting tools to spend time discussing their perspectives and add to or challenge our growing list of security issues as they evolved.

We would like to acknowledge and thank the following for their time and thoughts on this important subject.

- **Dr. Vint Cerf,** Chief Internet Evangelist, Google
- **Kirit Amin,** Chief Information Officer, U.S. International Trade Commission
- **Stephen Schmidt,** Vice President, Security Engineering; Chief Information Security Officer, Amazon Web Services
- **Syed Zaeem Hosain,** Chief Technology Officer and Founder, Aeris Communications, Inc.
- **Daniel Obodovski,** Co-author of *The Silent Intelligence: The Internet of Things*
- **Lin Wells II,** Managing Partner, Wells Analytics LLC; Former DOD Chief Information Officer
- **Maureen Ohlhausen,** Commissioner, U.S. Federal Trade Commission

4 WHAT IS THE INTERNET OF THINGS

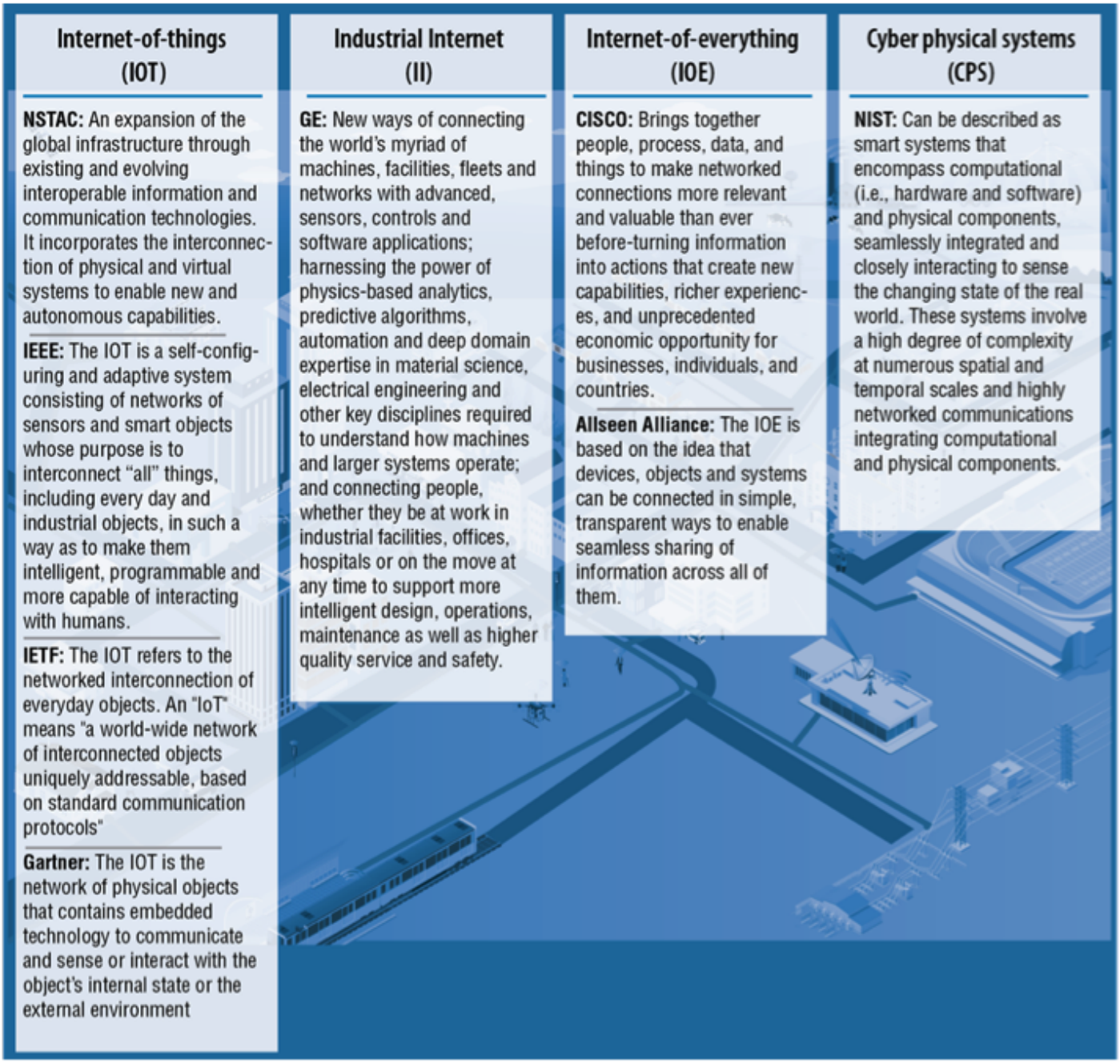
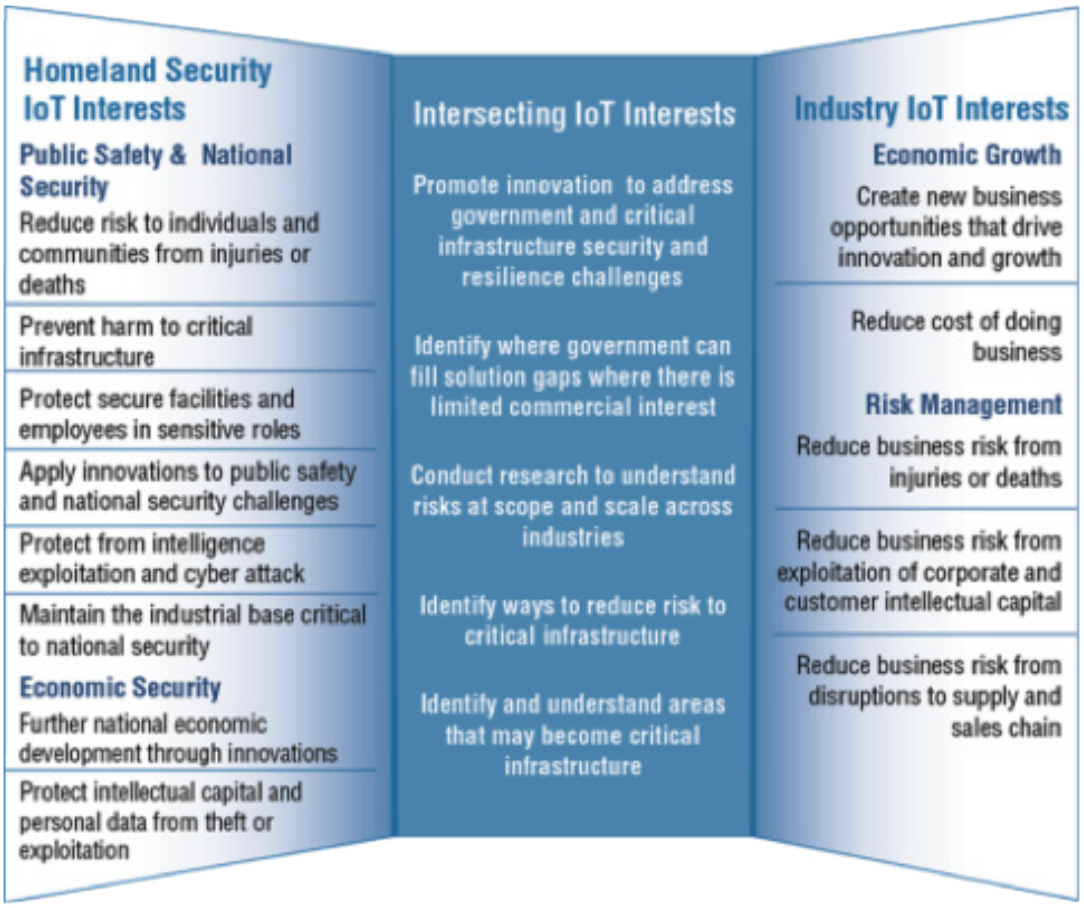


Figure 4-1, What is the Internet of Things Depends on Your Perspective

continued >

Defining the IoT is like trying to define…well, "you know it when you see it!" Depending on where the readers sit shapes their thinking, their perspectives, and their very emotional reaction to this topic (see Figure 4-1). However, all the hype devoted to this topic seems to boil down to a few key ingredients. The IoT is physical, connected, and smart. The IoT is to the Internet what the Internet was to word processors.



What do we mean by the IoT being physical, connected, and smart?

Physical: It is, at its essence, everyday devices used by people and organizations to manage their lives and business.

Connected: Networks connect devices to each other and to shared data and processing services. They also connect their users to one another.

Smart: Devices, services, and even networks continually sense, share, and analyze data and information to enable autonomous or semi-autonomous action.

Regardless of the myriad of definitions and views held, the U.S. government and its partners in the national and homeland security communities are going to be confronted by a reality that places the IoT squarely in their offices and environments, and it will impact their missions. Beyond the obvious threats these new devices bring to the cyber ecosystem, departments and agencies will confront the need to address threats and vulnerabilities existing in their current public-facing network presence, as well as untold threats that the smart, connected, physical components potentially pose. Reports on the projected value that the IoT has specifically for the public sector include the ability to increase employee productivity, improve military connectivity, reduce operating costs, enhance citizen experiences, and boost revenue.[3] Those government agencies responsible for defending this new frontier, such as DHS and DoD, will face additional challenges. In its role as the executive agent for securing the ".gov" domain and working in partnership to help industry to secure the ".com" domain, DHS (and its homeland security partners) have some large hurdles to clear.

[3] http://www.informationweek.com/government/leadership/internet-of-things-8-cost-cutting-ideas-for-government/d/d-id/1113459.

5 EVOLUTION OF TECHNOLOGY AND CONVERGENCE

Technology continues to evolve and change. It interacts and intersects with us in new and exciting ways with each new generation. The technology of today not only promises to bring with it untold promise but also unforeseen challenges. In some ways, the IoT presents known risks long associated with information security, including data loss, physical impact of cyber-attacks, and poorly protected targets. However, the scale of interconnectedness across so many discrete products, services, and systems also leads to different risks. Some of these differences are from increased consequences of known risks. Other differences emerge from risks acting in combination with each other in new ways.

continued >

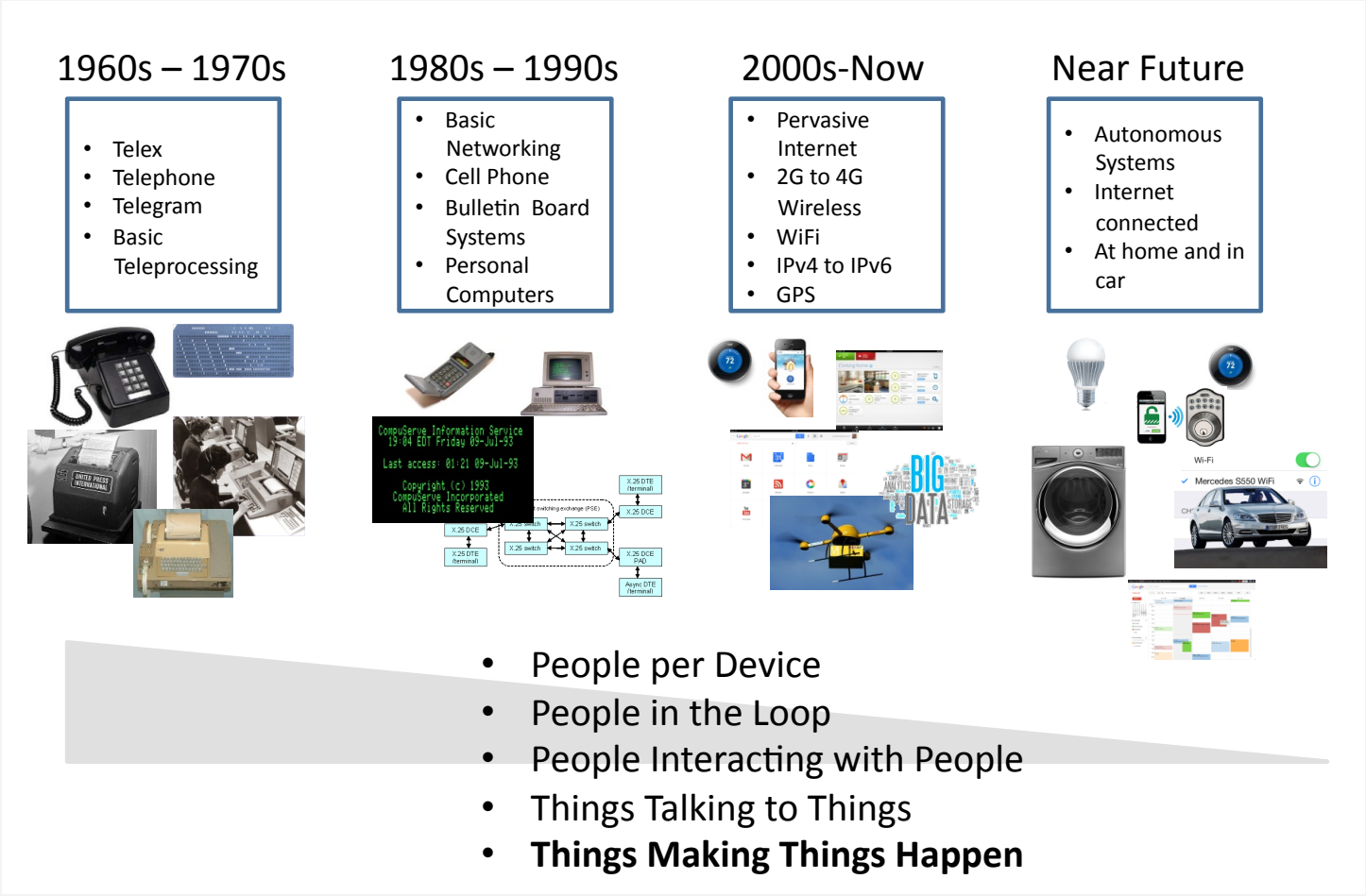


Figure 5-1, Evolution of Connected Systems and System Convergence

Shown in Figure 5-1 is a representation of the convergence of systems and the changes in how systems related to system and users relate to those systems. The general trend is that we have moved from systems where there are multiple users (or people) per device, people in control loop of the system, and the system providing the ability for people to interact with people. The IoT transition puts this on its head, where there are multiple devices (or hundreds) per user; the devices are things that are predominately talking to things; and the interaction is not just with users, but with real physical effects (*e.g.*, lock doors, turn on lights, change room temperature). Of course, the Internet is the common convergence network capability, replacing the previous independent systems.

An excellent and timely example is the integration of Whirlpool's new home washers and dryers into the Google's Nest environment,[4] enabling the dryers to coordinate their cycle on whether the Nest thermostat determines you are home or not. So, now not only does Google know you are not home, but Whirlpool does as well. Bottom line, the cyber threat surface just doubled (not to mention the potential wrinkle surface by not immediately drying wet clothes).

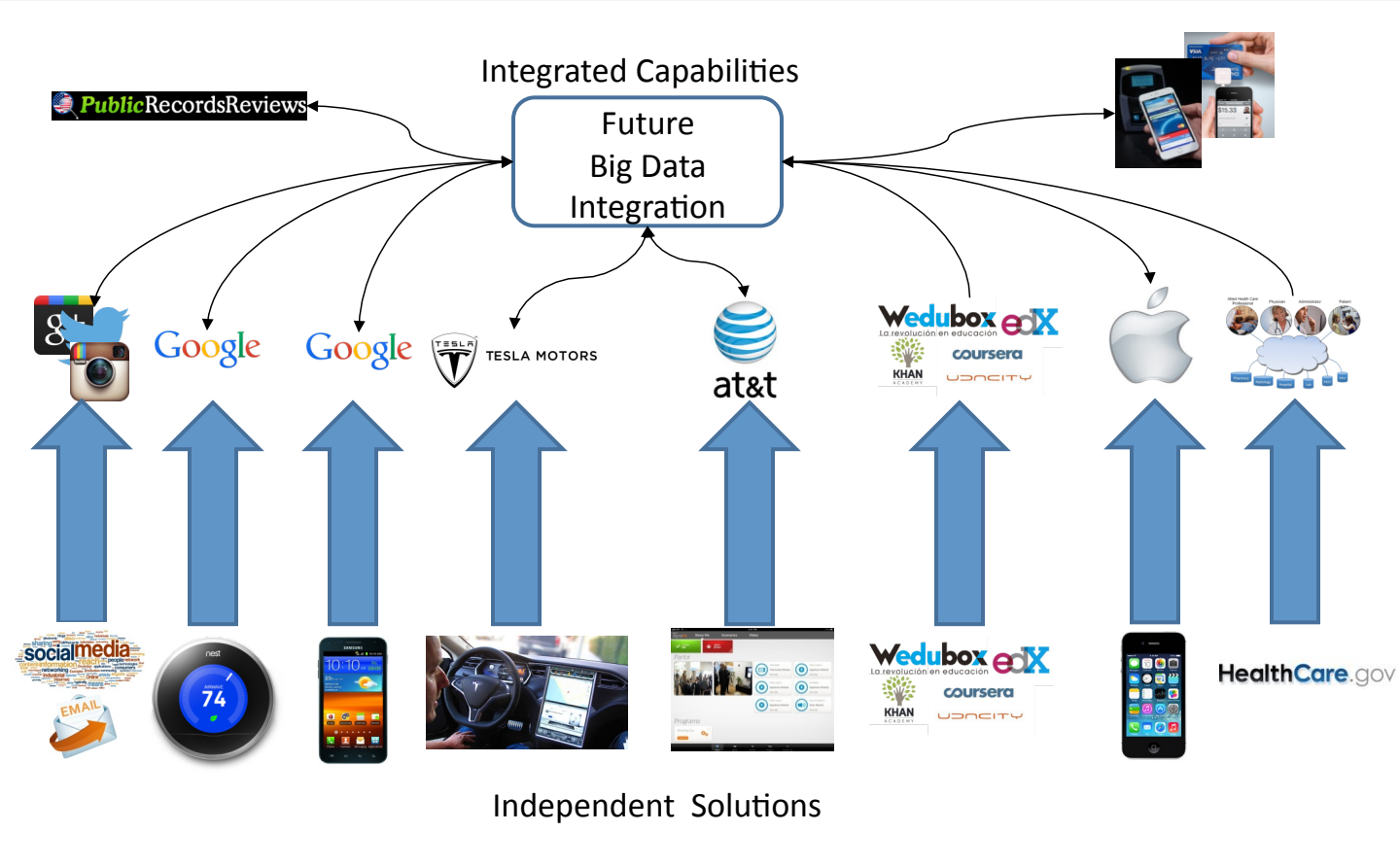


Figure 5-2, Data Convergence and Increased Risk

Data convergence, another aspect of convergence, is shown in Figure 5-2. The current stove-piped set of Internet services, and now IoT services, produce prodigious amounts of data. Some of this data are used to monetize search to direct advertising. However, risk to the systems and even to personal and public property may be increased significantly based on the likely correlation of multiple sources of data based on so-called big data analysis. The hypothesis is that, by correlating data from multiple sources, information can be used to hack or social engineer entry (*e.g.,* by impersonating the owner) into systems.[5]

[4] Techhive, *Whirlpool's new washers talk to Nest while you are away,* http://www.techhive.com/article/2864412/whirlpool-s-new-washers-talk-to-nest-while-you-re-away.html.
[5] CNBC, *'Anonymized' credit card data not so anonymous,* http://www.cnbc.com/id/102385271#.

6 EVOLUTION OF PRIVACY ISSUES[6]

6.1 U.S. Legal Aspects

Many complex issues can be analyzed, at least initially, by looking at technological, procedural, and personal aspects. It is generally accepted that technology outpaces the other two aspects. This clearly is the case with the burgeoning IoT, where technological developments have occurred faster than the procedural approaches to deal with them (*e.g.,* government regulations and industry-championed voluntary guidelines), or the personal aspect (*i.e.,* individuals and training for them).

The greater connectivity occasioned by the IoT will also ratchet privacy concerns to even higher levels than heretofore. The consequences of failure to maintain privacy successfully will affect peoples' lives more intensely than the consequences heretofore associated with their experiences with computers for email and work, as well as their status such as medical patients or financial clients.

The Constitution and Bill of Rights do not expressly set forth any right to privacy; however, the U.S. Supreme Court has found a right to privacy through its interpretation of the First, Third, Fourth, Fifth, and Ninth Amendments.[7] The concept of privacy as a legal interest was first enunciated in an article co-authored by Samuel Warren and Louis Brandeis in 1890, who described it as "the right to be let alone,"[8] which implies conscious decision by the person involved.

Privacy achieved hallmark status as a federal government issue with the enactment of the Privacy Act of 1974 (The Privacy Act). The Privacy Act required agencies to identify systems of record and permitted uses of those records—most of which were still in hardcopy form in the mid 1970s. The Privacy Act applied only to federal agencies, not the private sector. State governments separately enacted Privacy Acts for records they maintained.

Subsequent federal laws and implementing regulations followed along sectorial lines [e.g., the Health Information Portability and Accountability Act (HIPAA)[9], which protected health information; the Gramm-Leach-Bliley Act (GLBA)[10], which covered consumer non-public financial information; and the Sarbanes-Oxley Act of 2002[11], which addressed corporate accounting information, all of which imposed security and privacy requirements for health, financial, and accounting data and generated a growing range of privacy plans, policies, and procedures. Additional federal laws addressed certain categories of information, for example, the Children's Online Privacy Protection Act (COPPA), and imposed privacy requirements across all industry sectors obtaining or managing this type of information. Finally, regulatory agencies, such as the U.S. Federal Communications Commission (FCC) and U.S. Federal Trade Commission (FTC), also imposed privacy requirements concerning consumer data.

At the state level, often conflicting views shaped the development of the law. One perspective focuses on the aforementioned impact of the electronic age on personal privacy. Another concerns the ongoing campaign to enhance security, particularly in the face of terrorist attacks. Obviously, a variety of federal and state laws cannot be the most effective means to address the privacy issues involved, especially from the perspective of businesses with multi-state or multinational operations.

continued >

---

[6] Some of the discussion here derives from research and participation in drafting several ABA publications in the early 2000s. Jody R. Westby, ed., *International Corporate Privacy Handbook,* Pre-Publication Draft, American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, August 2003.

[7] "Development of the Right to Privacy in Information," http://www.csu.edu.au/learning/ncgr/gpi/odyssey/privacy/orig_priv.html (from the U.S. Congress, Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information,* OTA-TCT-576, U.S. Government Printing Office, Sept. 1993) (hereinafter "Development of the Right to Privacy in Information"); *see also* Electronic Frontier Foundation, *http://www.eff.org/Legal/email_privacy.citations* for a series of citations from U.S. court cases regarding constitutional rights to privacy.

[8] *Id*. Warren and Brandeis borrowed the term "the right to be let alone" from the Michigan jurist and 19th century legal scholar Thomas Cooley. *See* Thomas Cooley, *Law of Torts,* 2nd ed., Vol. 29, 1888.

[9] Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191, http://aspe.hhs.gov/admnsimp/pl104191.htm.

[10] Financial Services Modernization Act of 1999, Pub. Law 106-102, Nov. 12, 1999, 15 U.S.C. Section 6801 *et seq.,* http://www4.law.cornell.edu/uscode/15/6801.html (hereinafter "Gramm-Leach-Bliley Act" or "GLBA").

[11] Sarbanes-Oxley Act of 2002, Pub. Law 107-204, Sections 302, 404, http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf.

Over the most recent 15 years, governments at all levels have characterized the privacy issue using such terms as personally identifiable information (PII). Industry has generally not used the term PII, although government regulation of the private sectors' data systems and information otherwise characterized as PII has increased.

With this thicket or hedge row of laws and regulations governing privacy in government and the private sector, one would think that privacy is well-cared for. However, as noted previously, technology takes the lead ahead of process and individuals. The still raw cyberattacks on Sony Pictures underscore how inadequate privacy safeguards remain.

> ***The players and institutional biases here are interesting to observe, though. The movie industry as a group is loath to take international relations into consideration and objects to regulation in all its forms. Thus, a movie that non-show business types might see as a direct slap in the face or taunting generates a cyberattack by a rogue nation. The industry then laments that government's (read intelligence community's) efforts to confirm attribution is taking too long. Finally, when the industry decides to pull the movie, loud voices are heard on one hand complaining that "America's caving" and on the other that the government should "do something."***[12]

6.2 Roles of Age, Gender, Global Region, & Religion

The IoT has benefited, and in the future even to a greater extend, from the global roll-out of IPv6. IPv6 provides an exponentially large number of addresses and has moved the Internet experience from a highly limited resource to an endless number of unique addresses that now can be assigned to the world. Pent-up Internet offerings limited by IPv4 now have full flight; therefore the most expansive ideas and offerings are only now rushing to the market place. Global IPv6 was not initially deployed as broadly in the U.S. markets as it was in other parts of the world. Some would even say that the United States has lagged in its IPv6 rollouts because many of traditional IP resources were controlled by the United States, and therefore the need for IPv6 was not as urgent. The point is that IPv6 and the expansion of the Internet are a global experience, and therefore so is the IoT.

For this reason, for security and privacy issues, it is wise to consider the implication of gender, global regions, and religion as we set in-place the overall structure of the IoT. Most countries of the Middle East have forms of governments that are intrinsically connected to the dominant faith of the region. Government laws are rules by the basic dogma of that faith. It is naïve of Americans to believe that the Internet and its governing policies can be divorced from these processes. IoT should be no exception.

As a global set of services, the IoT and its related collection of data will be governed by legal concepts that are currently outside of U.S. law (but impacts U.S. companies[13]). A good example of this is the "Right to be Forgotten"[14] discussed later in Section 8.5.

Of course, legal, regional, and cultural impacts are important; so are the other forces that act on high-profile groups. For example, celebrities are now using old-fashioned flip phones to counter the security concerns of having devices that have increasing exposure because of the complexity of services (including IoT) they provide.[15]

---

[12] Dan C. Hurley, December 2014.
[13] The Guardian, *EU to Google: expand 'right to be forgotten' to google.com,* http://www.theguardian.com/technology/2014/nov/27/eu-to-google-expand-right-to-be-forgotten-to-googlecom.
[14] techdirt, *EU Things It Has Jurisdiction Over The Global Internet: Says Right To Be Forgotten Should Be* Global, https://www.techdirt.com/articles/20141127/07211929267/eu-thinks-it-has-jurisdiction-over-global-internet-says-right-to-be-forgotten-should-be-global.shtml.
[15] CBS News, *High-profile stars find fashion in old-school phone tech*, http://www.cbsnews.com/news/flip-phones-making-comeback-with-celebrities-and-fashion-icons/.

7 EVOLUTION OF PUBLIC POLICY

We have all come to expect and fully anticipate the rapid evolution of technology. High technology companies repeated re-invent themselves, seemingly on a daily basis. Technology evolves so quickly that the American appetite for changes in technology appears to be insatiable. However, a collateral piece of technology is also rapidly changing, and that—privacy— receives only cursory attention. A generation of Millennials yearns for new advances in the latest Apple iPhone applications and releases but appears to have less concern for the inherent issues of privacy and security that should, and must, evolve with those technological advances. The first generation of Americans that essentially grew-up on Facebook has never really reconciled the demand for instant personal information that fuels social media with the risks associated with violations of privacy and therefore personal security. This socio-economic sector is not demanding to know how its privacy is being addressed and protected. Applications designers and providers do not see this factor as purchase criteria. Software and systems are simply sold under the general heading of *caveat emptor* or "let the buyer beware." Is this truly enough? Traditional sources of protection (such as the FTC and FCC) are not directly involved perhaps because of the rapidness of the technology evolution. These traditional regulatory sources only intervene after a critical event emerges and public safety surfaces as an issue.

In the years past, enormous energy was placed on protecting a citizen's privacy as it relates to U.S. Postal Service or telecommunications providers such as the Telecom Act of 1934, updated in 1995. Mail fraud and any act of violating a citizen's privacy using traditional mail have serious federal law consequences. But the protection of the citizen when dealing with digital mail and information lags behind the technology advances. The law and the process of adjudicating violations are vague.

As machine-to-machine communications (M2M) such as IoT expands to the levels predicted, the role of the citizen and the role of the provider need to be more clearly defined. Where exactly should the lines be drawn between the responsibility of consumers to protect themselves via such means as passwords or physically securing assets and the inherent role of the service provider?

Amazon offers a working model (see Figure 7-1) where these roles begin to be defined, at least with respect to cloud resources. The key point is not whether this model is right or preferred, but that the need exists for a more public discussion about a common model, so consumers enter into these important relationships with clear expectations and knowledge of known risks.

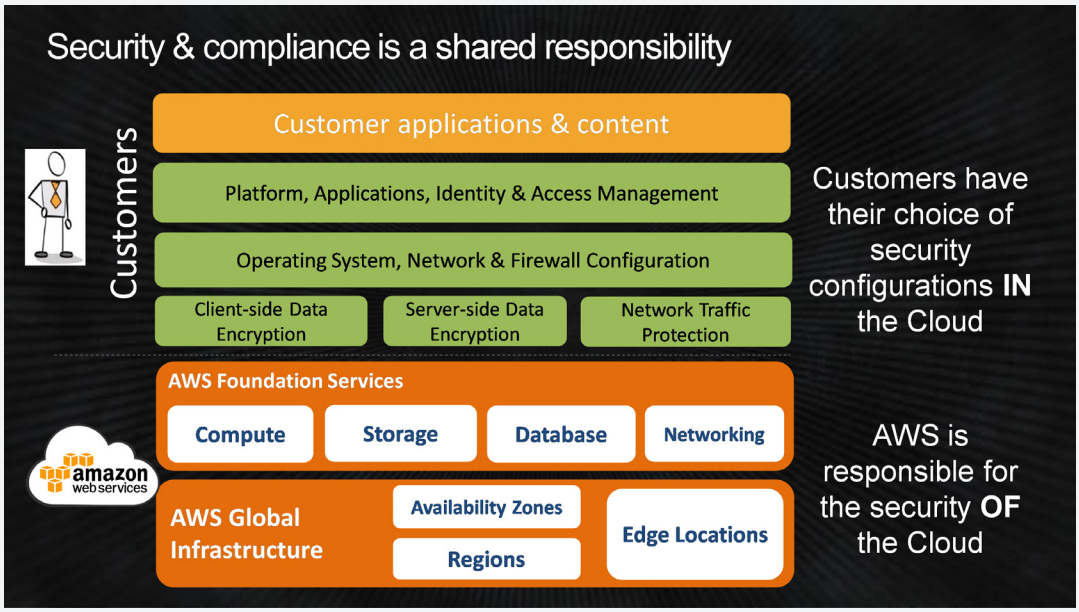


Figure 7-1, Example of Shared Security Responsibility from Amazon Web Services' Perspective

We need a common ecosystem reference model such that the areas of identity, access management, and other areas of security can be addressed consistently across the IoT landscape.

8 HOT BUTTON ISSUES

We present our seven hot button items that guide some of our thinking and exploration for technical and policy approaches dealing with the emerging cyber threat.

8.1 Privacy

The number one issue related to the IoT is privacy. The technological developments that enable use of the cloud and the IoT are real, expanding, and here to stay. Efforts by governments, industry, and academia to provide processes for the effective and safe use of these developments clearly need further work. People, whether as individual users or as professionals in the information technology (IT) field, need to assume more responsibility, including training, with respect to their individual use, and to encourage more individuals to pursue careers as IT professionals. Privacy has always been traditionally an add-on feature incorporated into hardware and software such as firewalls and various anti-virus software products. IoT's level of connectivity is unprecedented, and with much of the interaction invisible to the user or owners, it is unprecedented in its potential vulnerabilities.

The opportunity exists to design solutions that include basic privacy and security controls. We cannot roll out IoT and then consider the implications of privacy and security concerns. It needs to be in the DNA of the solutions. The world is focused on privacy, and it is clear that the American view is different from other countries. Europeans have more stated concerns for their privacy with laws in many areas of Europe reflecting that concern. The British are leading the way in a debate commonly called "the right to be forgotten." This dialogue demands that vendors provide proof that certain records of activity containing their personal data are destroyed and/or permanently removed, not only from the public view, but also from within the providers' entire system. This represents an enormous burden on providers but may have to be considered in the design of offerings. This issue has a critical function within the IoT because the level of awareness IoT gains into traditionally private actions, such as your presence at home, your use of medicine, and your consumption of entertainment are all in the machine to machine world of IoT knowable.

Providers, system owners, and regulators need to understand the real privacy issues emerging with IoT and address them quickly—the IoT consumer (and business) boom is already in motion. Simply adding more clauses to the dozen or more pages of existing and completely incomprehensible software license agreements (usually designed to protect the service provider) is not going to be acceptable. Consumers should be provided with recourse to affect the use of their private information, and, in particular, the sale or use of their information by other providers.

Recommendation: The IoT industry needs to provide, intrinsic to its consumer products and services, clear, understandable, actionable, privacy control for the lifecycle of its customer relationship.

8.2 Security

The full range of security issues related to IoT is beyond the scope of this white paper. However, it is possible to demonstrate a measure of the complexity of the systems being deployed today. Figure 8-1, shows a major fragment of systems that are used today, with the example focused on home automation using smart thermostats.

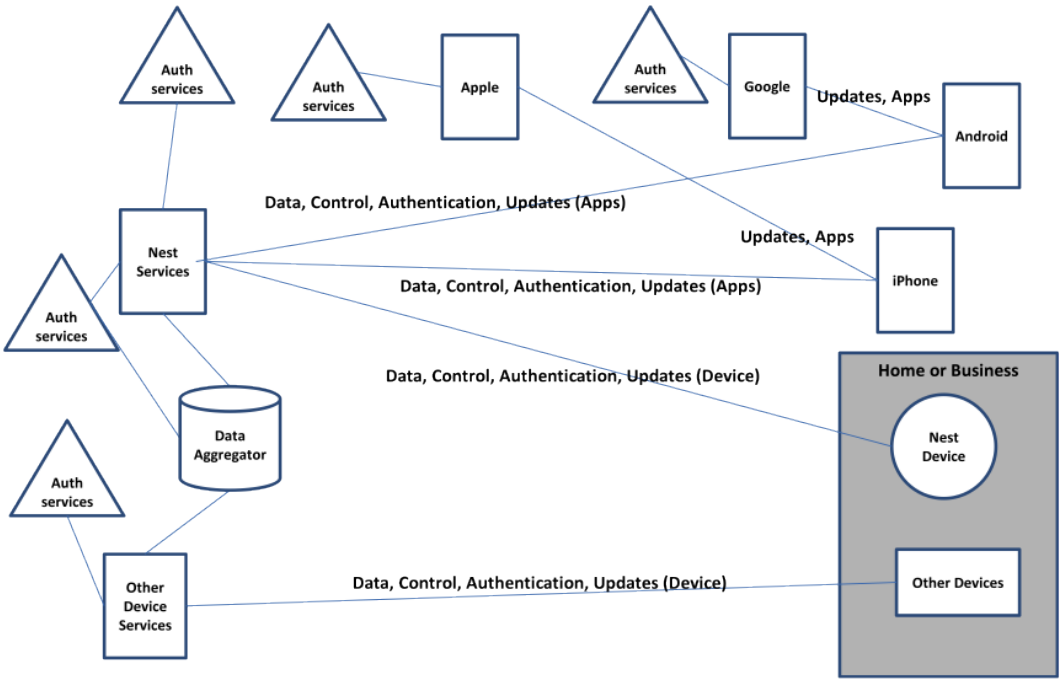


Figure 8-1, Current Security & Authentication Model

What should be noted is that several different ecosystems are working at the same time, each with its own security implications. The first natural question is to ask, "What is the security of the Nest[16] device or the Nest service itself?" However, we can see from the diagram that the Nest service interacts not only with itself, but also with services from Apple and Google. In addition, in some future state, a data aggregator may pay Nest or other home automation IoT provider for information to provide a yet completely new capability. In all of this, several questions are illustrative of the issues at hand. For each, we will give an example and a potential impact.

What is the Expectation of Security? In general, the user, without a lengthy examination of pages of license agreements, believes that the IoT system is secure in that only the service provider has direct access to the device in the home and that the establishment of a username and password with the IoT service provider is sufficient. Even if it is understood that another potentially hackable device has been placed on their home network, the expectation is that this does not create a back door into other devices on the home network.

In addition, the user expects that the service provider will maintain updates of applications that use the service. These include Web-based services, and more importantly applications that use other IoT devices for control, for example iPhones and Android-based (as well as others) phones.

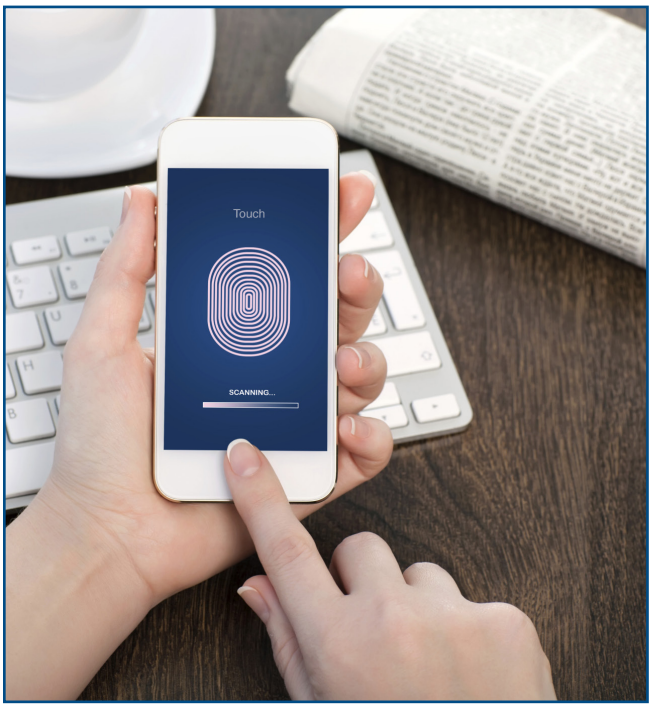
Unknown to the IoT service provider and the user is that the security status of their control devices is just as much an issue. Updates of these devices are an essential part of maintaining security of the system. For example, a security vulnerability in an Android phone may allow a key logger to be installed or enable the exploit of a weakness in a secure protocol[17] to obtain credentials needed to compromise access to the control of the IoT device, as well as enable access to IoT collected information. Again, it is the user's expectation that manufacturers and service providers of the IoT device and control devices will keep these devices up-to-date with near-invisible patching.

continued >

[16] https://nest.com/.
[17] For information on an example of vulnerability in the SSL protocol see, http://heartbleed.com/.

As will be discussed in Section 8.6.2, the long-term use of the device and its support by the manufacturer and service provider are serious security issues. More concerning is the possibility that devices are specifically designed to capture user login information right at the source. For example, a researcher developed what looks like an innocuous USB wall charger that actually cracks Microsoft wireless keyboard[18] and can send the information wirelessly to an attacker (or someone who will sell the information to a hacker). Hacking devices such as this could easily be inserted into the supply chain for distribution to hundreds of thousands (if not millions) of homes and business, creating a significant threat of identity theft and hacking of IoT users *en masse*. Without a counter espionage-type sweep (think James Bond) of a house, one might never know what really exists. Of course, what is worse is the possibility of an attacker hacking an existing devices and using it to create similar functionality.

More than a potential inconvenience for a home user, disruptions of services could include a coordinated terrorist attack by turning-on all air conditioners at the same time at the height of summer heat wave, potentially causing damage to the power grid.



Confidentiality, Integrity, and Availability. Users also have an expectation of confidentiality of the use of the system. The data held by the IoT service providers are for the use of the service provider alone. However, in many cases, after an exhausting read of the license agreement, it becomes clear that the IoT provider will most likely be able to do anything it wants to with the data, including selling the data to a data aggregator that will attempt another level of monetization. This is a common everyday occurrence and is a major source of Internet company revenue. For example, browsing a Web site for golf bags will inevitably mean that for the next several days, pages on browsed news sites will include advertisements for golf bags.

In the case of golf bags, confidentiality may not be of the highest concern, however we are now seeing devices that measure a person's health and their health-related habits. Clearly, the dissemination of this information, which with some effort most likely could be correlated to an individual, may start to spark significant concerns.

Data integrity may not seem to be a significant security issue. What the temperature at a user's home was for a date in the past may not seem like an important issue. However, like a person's credit score, as more and more information about a user's life and habits is captured, how will that impact his or her professional reputation, or on the performance of other IoT systems that used the data provided by another IoT service provider?

Another aspect of security is system availability. The ability for the systems to defend against denial of service (DOS) attacks is critical as a whole chain of dependent systems may be affected. This is a real concern as the recent attacks on Sony's PlayStation network and Microsoft's Xbox Live show that a small group of hackers can impact the availability of the service.[19] More than impacting game play, this also impacted the ability to use the gaming consoles for buying and watching movies. No doubt this is a significant impact on commerce and proves that even long-established systems run by well-known companies are vulnerable.

continued >

[18] VB News, *This USB wall charger secretly logs keystrokes from Microsoft wireless keyboards nearby,* http://venturebeat.com/2015/01/12/this-usb-wall-charger-secretly-logs-keystrokes-from-microsoft-wireless-keyboards-nearby/.[13] The Guardian, *EU to Google: expand 'right to be forgotten' to google.com,* http://www.theguardian.com/technology/2014/nov/27/eu-to-google-expand-right-to-be-forgotten-to-googlecom.

[19] BBC News, *Xbox and PlayStation resuming service after attack.* http://www.bbc.com/news/uk-30602609.

Consumer Awareness. Virtually no consistent awareness exists among consumers regarding the impact that IoT devices can have within their homes. Several factors to consider are:

- The assumption that IoT services will be patched and that security is someone else's responsibility;
- The compromise of millions of username, passwords, and credit cards with few very public horror stories of how a hack attack ruins reputations or impacts homes; and
- The mixed messages from the government on the real severity of cyber malfeasance [*e.g.,* the U.S. government's response to attacks, and in particular the recent hack (or inside job) of Sony Pictures, being characterized as an act of cyber vandalism.[20] Although, it may not be an act of war (even if it was sponsored by the North Koreans), if an organization broke into a bank and took negotiable bearer bonds from the vault, we doubt the government would call that breaking and entering event an act of vandalism.

Consumers are becoming numb to the potential impacts of their increasing use of IoT services. With mixed responses from government, it is hard for the IoT industry and customers to care.

Liability. Ever since (or almost contemporaneous with) the first user license agreements, IT providers have tried to hold themselves harmless for any damage caused using their equipment. Barring settlements from periodic lithium battery combustions, we currently use IoT devices and services at our own peril. However, these agreements were based on devices that only had a logical impact on our lives (*e.g.,* lost email or corrupted files), not on physical action (e.g., turning on lights, HVAC, security systems, and cameras, or unlocking doors).

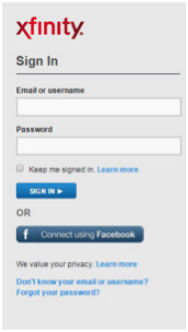
However, this may change as IoT devices and services are now being used to commit illegal surveillance that brings a new dimension to stalking.[21] It is only a matter of time until this will reach to IoT home devices. In fact, there may already be a case of using IoT as a method of revenge, where a spurned husband used an Internet connected home thermostat to wage temperature retribution against his wife.[22]

Will the physical action-at-a-distance reality of the IoT lead to liabilities being placed on IoT device manufacturers and services providers and the development of a new insurance market?

Recommendation: IoT development must include security without effort as virtually no consumer is an IT security expert. This must include the interplay between device ecosystems—users cannot be expected to perform positive actions to make up for security flaws.

8.3 Identity Management

One of the fundamental aspects needed for security for IoT (and for that matter many Internet-based services) is the ability to identify, with certainty, users or devices that make up the system. For most Internet services, especially the free ones, there is no confirmed identity of a user. For other systems, the identity is based on either a bank account or credit card verification.



However, with a proliferation of services comes a proliferation of identity systems. For example, one Internet service provider, Comcast's Xfinity, enables individuals to use their Facebook account as identity for signing-in to the Xfinity services and management Web site. The vulnerability here is obvious, and, in the very least, it doubles the opportunity for a hacker to obtain login credentials of an account. Of course, Xfinity is also an IoT provider, and associated with your account is the ability to add home security and home automation. With a compromise of a Facebook account, someone could come home after vacation to find his or her house cyber vandalized (with the heating system turned-off potentially causing the pipes to freeze) and/or to receive a follow-up phone call from the vandal (who now knows you are home because he can see you on your own security camera).

continued >

[20] Reuters, *Obama says Sony hack not an act of war,* http://www.reuters.com/article/2014/12/21/us-sony-cybersecurity-usa-idUSKBN0JX1MH20141221.
[21] UK The Independent, *Exclusive: Abusers using spyware apps to monitor partners reach 'epidemic proportions',* http://www.independent.co.uk/news/uk/home-news/exclusive-abusers-using-spyware-apps-to-monitor-partners-reaches-epidemic-proportions-9945881.html.
[22] Opposing Views, *Amazon Reviewer Tells How He Used a Product To Get Revenge On His Wife,* http://www.opposingviews.com/i/society/amazon-reviewer-tells-how-he-used-product-get-revenge-his-wife.

In addition to identifying users, IoT providers must have a system that enables them to identify their devices and for the device to identify the provider. In general, this is done using Public Key Infrastructure and is used to set up trusted connections between the device and provider for patches, software upgrades, and information exchange. Security here is maintained to the extent that the IoT manufacturer and service provider have good code and maintain good key discipline. Of course, how did they establish identity in the first place?

Recommendation: We need to rethink the approach to identity. For example, is there a role for government? Specifically, can U.S. Postal Service provide an identity vetting service?[23]

8.4 Digital Divide

The digital divide does not mean merely the difference between the "Haves" and the Have-Nots." The broadest definition includes those with disabilities, literacy issues, the elderly, and those non-English speaking users. Even the homeless should be given some consideration because many states provide digital access as a mean of distributing benefits. As stated earlier, we are at the architectural design stage of the IoT. It is at this stage that we can design a platform that considers these broader perspectives. That is not to say that every need has to be met or every situation anticipated. The call here is for inclusion wherever possible by design and not as an after thought. The IoT could broaden the digital divide, but it could also provide creative solutions to traditional problems in education, health, housing, energy, jobs etc. There is a need to position IoT as broader than a marketing campaign or product up-sell.

Recommendation: Standards groups should be required to explicitly demonstrate plans to make the technology of IoT accessible to those with disabilities including the blind, deaf, and hard-of-hearing. Pricing schemes and offerings must have plans that offer the basic service to those at a variety of earning levels. The cost of mitigating identity and abuse of IoT should not automatically fall to the consumer. Some element of regulatory review should be a given factor in IoT public service offerings.

8.5 Ownership of Data

One of the cornerstones of the Internet business model is the collection of data that can be used to create new revenue streams. It is this business plan that leads to directed advertisements on Web pages and the fantastic valuations of companies such as Facebook and Twitter.

This leads to some questions that will have to be resolved.

Monopoly and Anti-Trust. As the ecosystems for IoT consolidate, when do we start moving into a situation where these companies start acting as monopolies of IoT control or data aggregation? If you are an IoT service provider, are you compelled to sell your data to a competitor in the data integrator space?

Ownership of Data. The real question is who owns the data? By using an IoT service, are you giving up the rights to the information collected about your house? Laws protect a person's personal health information (*e.g.,* HIPAA Security Rule[24]) but do these apply to the health related information collected by personal activity trackers such as Fitbit, the heartrate information collected by your Samsung Galaxy 5, or the exercise and diet information in the Apple Health app?

Is this data something protected by the U.S. Constitution's Fifth Amendment, or is it meta data that can be requested by government on demand?

Barriers to Exit. What can you do when you no longer want to use the service? What happens to the data? Can you request to be forgotten? If the IoT provider supports your request, does it extend to the companies where it sold your data previously? In Europe, there is a "Right to Be Forgotten."[25]

continued >

[23] Kaplow, *Post Office Future Redux,* http://kaplowtech.blogspot.com/2011/09/post-office-future-redux.html.
[24] HHS, *HIPAA Security Rule,* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/.
[25] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

Moving to Different Providers. If you own your IoT data, can you take it with you? Can you move from one provider to another? Most commercial email services, those that have a subscription cost, allow accounts to be archived. Once archived, the account data can be moved to another provider. Some heavy lifting may be required to import the data into the new system, but in most cases this is made possible by the email service providers or third party tools.

Does this concept apply in the IoT universe? Is the data held by a previous provider important, or is anything more than a few months old simply not worth anything to the user?

Recommendation: Standards must be created that define data ownership. The typical default action that tacitly gives permission for data use in ways never envisioned cries out for commercial self-regulation. If that doesn't happen, government intervention will likely follow.

8.6 Operational Issues

The lifecycle of an IoT system has many perspectives based on the roles of those making, operating, and using the system. Table 8-1 summarizes these various roles and associated operational expectations and perspectives.

Table 8-1, Operational Perspectives

Role	Expectations	Issues
End-User	• Ease of use • Privacy of information • Security of the system • Personalized • Easy availability of collected information in a format easy to use	• Unknown privacy impact • Unknown security status • Maintenance of username and password • What is the relationship with the administrator? • What is the authentication method with the administrator?
System Administrator	• Simple administration • Will conform to existing security environment • Strong authentication of system administrators • Can be incorporated into an enterprise's identity and access control system • Can escalate problems with the provider	• Unknown security implications on internal networks • For home users, this is generally a non-technical user • What is the relationship with the provider? • What is the authentication method with the provider?
Service Provider	• Rapid deployment of service end-to-end system • Minimize support structure • Gathering of data from IoT devices to provide service to the device user, as well as potential monetization of the information • Wants to introduce new devices and services to expand market share	• May not use best cyber practices in the creation of the system • Supporting the setup of the system with the administrator • Maintaining the relationship with the administrator • Eager to make money, business plan probably includes selling data • Must maintain support of older devices and system, even after they may not be supported by the maker
Maker (Manufacturer)	• Make the IoT devices as cost effective as possible • Leverage existing codes bases for new devices • Rapid development and sale • Rapid obsolescence to drive sales	• Support for old devices is a cost issue • Common code basis equals common mode security vulnerabilities
vData Integrator	• Looking to mine data from multiple service providers • Does not require a relationship with the actual IoT users	• Trust that the IoT service provider does not send certain information to the data Integrator based on privacy norms or regulation • Data Integrator can leverage multiple data sources and feeds that can be used to identify IoT users in ways that the user never intended to be public

Recommendation: Reasonable and customary care definitions for providing services in IoT space, at every level of service use and creation, need to be defined. This is critical to establishing the foundation of potential legal liabilities for issues related to IoT.

8.6.1 User Perspective

There are several different cases to explore when examining the user perspective. The user can be the end-user, a corporate system administrator, or a system provider operator. Of importance is that these are not mutually exclusive. That is, an IoT system may at the same time provide an end-user experience while a system administrator supports the system.

When it comes to the user experience, several items are of particular note:

- What is the digital debris that is left from all these devices and services?
- What is the difference between the first user of an IoT device or service and the next user?

Passive digital debris is the digital information that we leave around us in increasing quantities and at an increasing rate every day. This is from search histories, Facebook updates, Tweets, documents libraries, iCloud, Google+, and the like. Although attached to some level of your identity, it is generally not attached to a device that you own or sell, such as those that might be in your house. However, with file synching such as Google Drive, Apple iCloud, and Microsoft OneDrive, devices may have cached passwords.

IoT devices create something new: *active digital debris. Active digital debris* are ensembles of those devices that become part of the long-lived infrastructure of a structure (or, could be devices in a car, for example). Take the case where several generations of IoT thermostats, refrigerators, lighting systems, an irrigation system, a security system, and video cameras exist. The original user who installed and configured the system understands (or thinks he or she understands) their use. What happens when the house is sold? What happens if the owner is no longer available? What happens if the owner does not remember how the systems are configured or their passwords? In fact, without an "IoT House Inspection," how would a new homeowner even know what is lurking in the light bulb next to her bed?

So, there are significant questions on how IoT systems transfer from owner to owner. What are the responsibilities of a user to clean up active digital debris? Without exaggeration, within a few years, there will be tens or hundreds of millions active devices within homes, cars, and businesses that are essentially running against their last set of configurations, unknown to the people they surround.

The User perspective for IoT is complex, trading ease of setup for end-users and administrators with complexity of network security and identity management for easy access to information. In addition, we tend to focus on the first owner and user of an IoT system and not what it means for the next user.

8.6.2 Maker, System Provider, and Total System Lifecycle

The IoT land-rush has the old-traditional, new-traditional, and fast-to-market startups all trying to stake their claims. Old traditional companies such as telecommunications and cable companies are trying to provide additional value-added services such as home automation to their portfolios. New traditional companies, such as Google, are developing (or buying-up fast-to-market companies) IoT systems. Finally, fast-to-market companies, such as Cozify, are trying to bring-out products as quickly as possible to build a user base, grow the company, and then potentially cash-out by being acquired.

Although a 21st century invention (clearly some will claim not), and not from the previous personal computer wave that put devices into the hands of hundreds of millions of people, IoT still has the same problems that many people have with their personal computers and smart personal devices. That is, the start, middle, and the unfortunate end of a system's lifecycle. Not a week goes by that an operating system or application provider—whether it is Microsoft, Apple, or Google—does not provide a patch to improve the user experience or more often to fix security-related issues.

At the beginning of the lifecycle of an IoT product or service, the expectation is that the developer is paying close attention to what can be broadly termed quality control. This quality is not only in the user experience, but also in the aspects of security and maintainability. Traditional companies, in general, have set development standards and quality assurance organizations and processes. However, for the fast-to-market companies, it is not clear what testing, other than usability testing, is performed. Do they take the time for full security regression testing for each new device and software load?

continued >

Although both categories of companies leverage open source software, traditional companies are more likely to run through complete set of tests that could expose security vulnerabilities. And, what may become more important based on state-sponsored or corporate espionage are independent code reviews that identify latent back doors placed by developer insiders.

During the active life of a product or a service, the maker of the product will likely release patches and upgrades. However, a significant difference exists in the use modality and useful lifespan between today's typical devices and the blossoming IoT devices. For example, from a study in 2010[26] Americans keep their mobile phones for less than 24 months (although the more recent trend is increasing[27]). This is in contrast to the typical home infrastructure such as major appliances, thermostats, and lighting. Once these are installed, they generally last for a decade or more.

There is a significant workload and expense on the developer or system provider to support devices for extended periods of time. Even Microsoft ended support after 12 years for its Windows XP product. As consumers and business discard devices, the backwards support for older version of hardware can be deprecated, reducing the overall backward regression testing regime.

However, even in the disposable age of smartphones and tablets, some of these devices last longer than expected. With the pad rush started by Apple, dozens of Asia-based companies rushed to build inexpensive Android pads. Many of these devices are still in use today, with zero updates provided by the manufacturer as they are past their expected lifetime. In fact, Google apparently has stopped support for an estimated billion devices.[28] With the extensive use of open source software, what is the likelihood that millions of these devices do not have well known vulnerabilities such as Heartbleed?

We normally associate the automotive industry as one that has a significant set of internal development controls. However, these have failed in the recent past, such as the ongoing litigation based on ignition key defects at GM that has 462 claims for death[29]. With this, as well as other industry issues related to the performance of safety airbags, are we to expect near flawless industry execution of the development of cars (and other vehicles) with Internet-driven navigation, maintenance, and self-driving features[30]?

With this as background, it is not hard to predict the likely lifecycle of devices that are embedded in the very fabric of a home or small business (or even a large business). These Internet connected devices will live for a decade or more, some kept up-to-date for a period, but then as IoT manufacturers announce end-of-support for devices (if they can even determine to whom to send such an announcement) or just disappear from the landscape, these devices will live on with whatever latent vulnerabilities existed when support was terminated.

From start-ups with loose development processes, to devices abandoned by even major manufacturers, homes and businesses in America will be filled with thousands (or more likely millions) of devices that have been orphaned from patches, upgrades, and technical support.

---

[26] phoneArena, *American replace their cell phones every 2 years, Finns – every six, a study claims,* http://www.phonearena.com/news/Americans-replace-their-cell-phones-every-2-years-Finns--every-six-a-study-claims_id20255.
[27] Bullfax, *Consumers are taking longer to upgrade their phones, another sign the smartphone revolution is maturing,* http://www.bullfax.com/?q=node-consumers-are-taking-longer-upgrade-their-phones-another.
[28] Forbes, *Google Under Fire For Quietly Killing Critical Android Security Updates For Nearly One Billion,* http://www.forbes.com/sites/thomasbrewster/2015/01/12/google-webview-updates-quietly-killed-for-most-androids/.
[29] Reuters, *GM gets 57 more claims for faulty ignition switch compensation,* http://www.reuters.com/article/2015/02/09/us-gm-recall-compensation-idUSKBN0LD1RX20150209
[30] Gizmodo, *Report Finds Anti-Hacking Car Security "Inconsistent and Haphazard,"* http://gizmodo.com/report-finds-anti-hacking-car-security-inconsistent-an-1684932752

8.6.3 Internal Controls

Previously, we discussed the concern over an insider threat during the development or maintenance of the software base of a system. Here, we are concerned about this as well as the internal controls of the service provider that is the recipient of the information provided by the IoT system. Where are the data generated by the IoT devices kept, and what are the internal controls of these companies to ensure that the data are only used for their intended purpose? What are the technical and personnel mechanisms used to ensure that data are properly handled?

Clearly, based on the recent number and magnitude of data breaches from large companies (see for example[31]), the track record for service organizations to safeguard information is less than stellar. With the threat surface dramatically increased by millions (or soon to be billions) of IoT devices collecting information as broad as "when people are on vacation," "whether their house door is locked," and "where they happen to be at the moment," the internal controls and audit of these controls will become more and more important as the value and scope of information are extremely attractive to organized crime.

Whether because of sloppy internal processes or the infiltration of developers or service providers by industrial or state actors, the opportunity exists for committing massive fraud and crime.

8.6.4 Information Exchange

The naïve may believe that information collected by service providers will stay with the service provider. Few if any people actually read the terms of service or privacy notices that govern the use of data. In general, users have become accustomed to the rapid targeted advertising associated with the use of Internet services such as free email, search, and Internet stores. Search for a digital camera on Amazon, and the next time you hit a news site, offers for cameras will abound.

This leads to the question of what is the responsibility of IoT service providers as they deliver information to other service providers. What is the responsibility of a service provider to ensure that the buyer of the information has sufficient controls to ensure that the sold information is handled correctly?

With the advent of big data analytics, these mega-repositories of IoT generated information, combined with the corpus of public Web information, means that over time, virtually every move, purchase, and communication performed will be able to be correlated down to a very personal level. What are the implications of this data and more importantly the company that collects and correlates this data for commercial purposes? Does this company have a significant liability, for example if a massive and organized burglary night occurs based on the distribution of information on targets of opportunity distilled from these massive databases?

Finally, with the emergence of pervasive cloud computing services in regions around the world, the data collected during these information exchanges may move from country to country. More than geographic change, this also represents a change in jurisdiction and law that may lead to information being used in ways that the originator of the data and of course the IoT service user never intended.

The massive collection of information, both from public sources as well as information based on the physical activities of users and people around IoT devices, leads to significant questions as to who is responsible as larger correlated personal information becomes invasive to people's lives.

8.6.5 Compatibility and Interoperability

At one time, several different digital mobile phone systems existed—TDMA, GSM, iDEN, to CDMA. Only GSM, a European standard, tried to make the handset free from lock-in to a particular carrier, with the identity of the phone tied to a chip that could be moved from phone to phone. Service providers thwarted this by locking phones to their network. Compatibility has driven essentially all providers to LTE, which has essentially made handsets universal to all providers. This compatibility means that consumers, once their phone is off contract, can have their phone unlocked and used for another service provider's network. It also means that a market exists for unlocked phones.

continued >

[31] Bankrate, *11 data breaches that stung U.S. consumers,* http://www.bankrate.com/finance/banking/us-data-breaches-1.aspx.

However, today this is not true with many IoT systems. They are essentially locked-in to the provider's IoT ecosystem. You can buy a Nest thermostat, but can you use another provider to control the device? Also, if you could, who would then be responsible for the update of the firmware in the device?

Without compatibility and interoperability, some set of available ecosystems consumers will be faced with devices in their homes and on their person that perhaps represent dozens of sets of ecosystems each with its own user management environment and each with its own data repository. In the worst case, you might have separate iOS Apps for turning the lights off in the bedroom, the family room, and the kitchen.

Like the mobile phone industry, the relationship between the ownership of a device and the ability to use that device in multiple service provider environments is key to reducing the exploding complexity of what a user faces in managing existing devices and adding new capabilities.

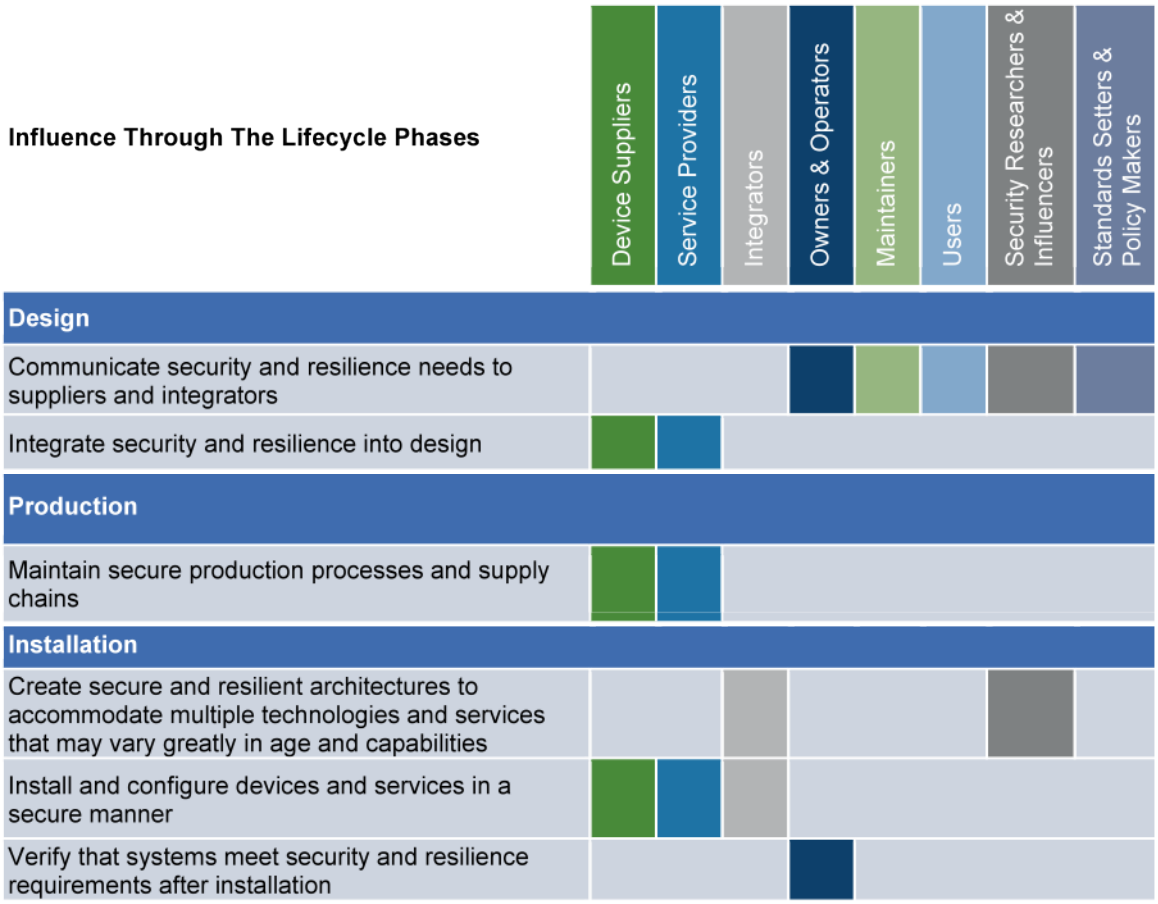
8.7 Leadership

Leadership in this area is a complex set of inter-related responsibilities, opportunities, and constantly shifting participants. In the early days of this, a combination of the traditional players and innovative upstarts will lead to the introduction of new individual products, with many of these more innovative being subsumed by the big players. Leadership will spring from where the center of mass begins. A deliberate, focused group of organizations such as international standards bodies, governance groups, and to some extent governments need to engage, actively and immediately. There is no escaping the need for strong leadership, those willing to put aside profit and stand shoulder to shoulder on shaping the technical and support required to move IoT from a series of colonies into a multi-national community.

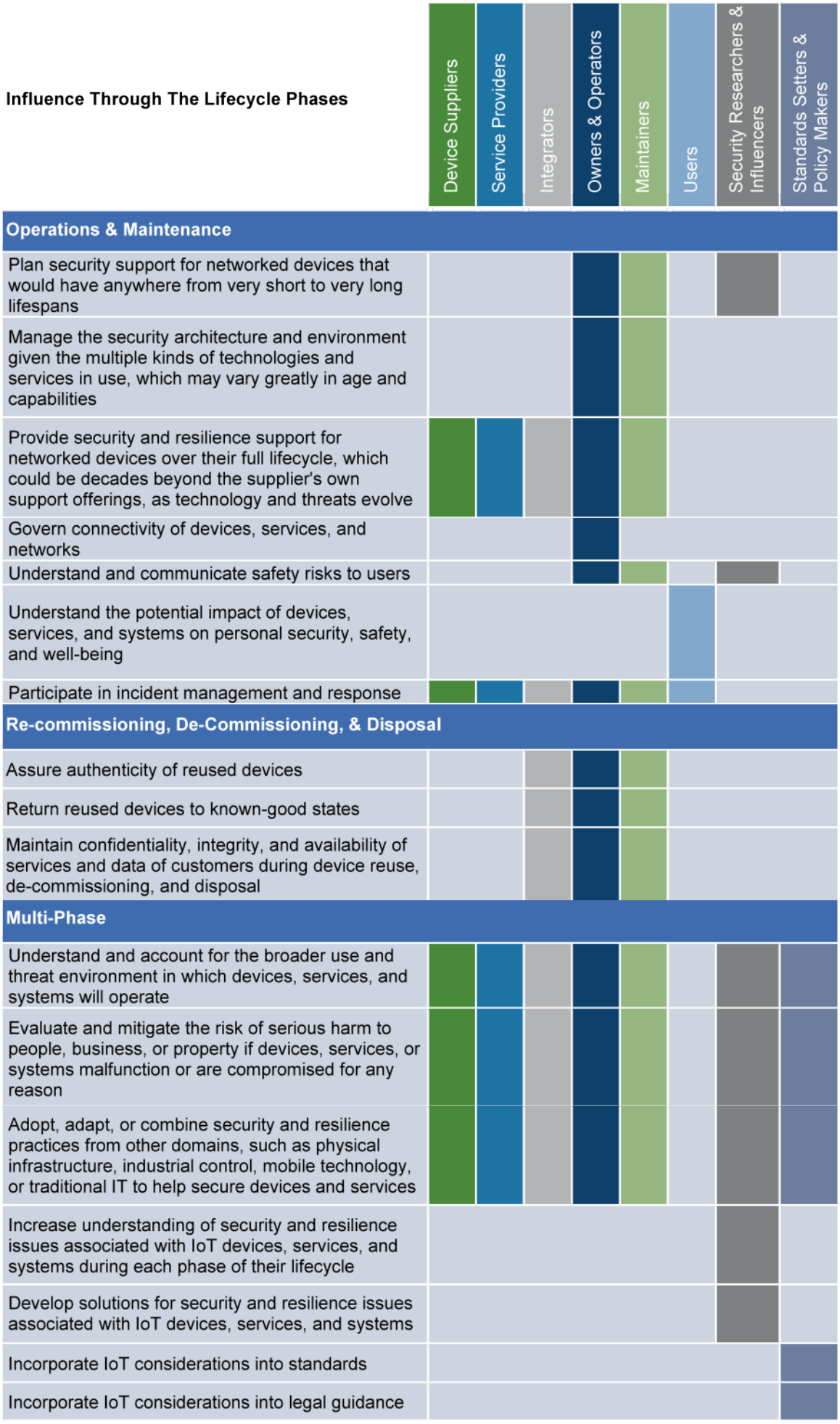
8.7.1 Need for Ecosystem Roadmap

In 2011, DHS called for a national conversation about the cyber ecosystem and methods to engage the cyber ecosystem in meaningful ways to enhance the security of our nation's critical capabilities. IoT needs such a national cyber conversation

continued >



Influence Through The Lifecycle Phases



and an accompanying characterization. Simply addressing the various elements of IoT in separate, stove piped manners will ensure that critical decisions being considered about the direction of this ever-changing ecosystem will fall to the same mistakes of the past. Below are some of the various stakeholders and influences that a national dialogue on IoT should begin to address.

8.7.2 Standards

In addition to the national conversation about developing an IoT ecosystem, a set of standards will need to be developed to address this burgeoning area. Standards have long been the best way for communities of interest to engage meaningfully, to work together to ensure common terminology, to develop mutually beneficial approaches, and to design elements that will work to support the entirety of the system rather than fracture and drive apart new technologies. Government plays a unique, but incredibly valuable, role in facilitating— but not owning—this portion of the mission. It often funds, encourages, promotes, and facilitates the development of communities of interest. The need for objectivity and purity in the early stages of the development of standards, as well as the need to act as a catalyst to provide the mechanisms to get these groups working together in mutually beneficial ways, are important areas for government to engage. Standards, languages, repositories, and now expressions of cyber threats, have been a constant source of unification in the cybersecurity ecosystem for almost 15 years. Uniting in common cause and purpose, industry, government, and trade associations alike have come together to develop, promulgate, use, and leverage these to define, frame, and shape the defense of systems and networks. Often, this is the one area where disparate organizations and competing organizations could come together, work in partnership, and achieve a common approach that transcends organizational ideologies and pushes the security of the ecosystem above the individual needs of the entities participating. It is safe to say that the Internet always has contained the DNA of standards. It is deeply ingrained in the culture of the Internet and the community that supports it. This deeply ingrained approach must be extended to IoT.

9 CONCLUSION

Not a day goes by during the final editing of this paper that another revelation in the media, either a news report of stolen information or a new product or service, does not drop right into one of our hot button items. What we do not see is the concerted effort to address the fundamental weaknesses of a new set of technical capabilities that is being unleashed into a public that is still challenged in maintaining the security of home laptops, pads, and smart phones. With the integration of action-at-a-distance capabilities, Elon Musk's concerns that artificial intelligence is a danger to humanity may be right on the mark. It may not be a robotic *Terminator*, but with control of cars, homes, and other industrial control systems, it may just have a similar effect.

The AFCEA International Cyber Committee White Paper Series

www.afcea.org/committees/cyber