Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

ISSUE BRIEF

Smart Homes and the Internet of Things

MARCH 2016 GREG LINDSAY, BEAU WOODS, AND JOSHUA CORMAN

The Internet of Things (IoT) is the next step in the evolution of wireless networks, Big data, and connected devices, as sensors shrink in size and migrate from our smartphones to other everyday objects. Analysts predict the IoT will double in size to nearly 50 billion things by 2020, comprising a $1.7 trillion market.[1] Some of these smart things already monitor the performance of power plants, factories, and jet engines; others collect our vital signs from bracelets and watches. In each of these cases, the IoT is both saving lives and transforming industries and societies.

One of the greatest opportunities still lies ahead in the form of the "smart home." Smart homes typically evoke visions of *The Jetsons'* robot maid or refrigerators ordering milk from Amazon, but they also offer possibilities for energy and cost savings, greater home efficiency through automation, as well as improved home security. Smart homes have the potential to provide for consumers' growing expectations of convenience, sustainable living, safety, and security.

Attaining these desired benefits, however, means these systems must deliver on consumer expectations. High profile security risks in IoT devices erode consumer confidence and adoption.[2] The analysis in this

The focus of the **Cyber Statecraft Initiative** is to examine the overlap of national security, international relations, and public safety to provide practical and relevant solutions to challenges in cyberspace. The Initiative works with Fortune 500 companies, governments, and other stakeholders to promote thought leadership in cyber statecraft—the key tool to generate innovative solutions for a free and resilient digital commons. The Initiative covers topics at the intersection of technology and the human condition, such as the impact of cybersecurity on public safety and economic stability and the growing importance of post-nationalism with the emergence of new, powerful actors in this sphere.

1 International Data Corporation, "Explosive Internet of Things Spending to Reach $1.7 Trillion in 2020, According to IDC," Press Release, June 2, 2015, http://www.idc.com/getdoc.jsp?containerId=prUS25658015.

2 Kashmir Hill, "Watch out, new parents—internet-connected baby monitors are easy to hack," *Fusion*, September 2, 2015, http://fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack/; "Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT," Capgemini, 2014, https://www.capgemini.com/resource-file-access/resource/pdf/securing_the_internet_of_things_opportunity_putting_cyber_security_at_the_heart_of_the_iot.pdf.

report draws attention to the delicate balance between this promise of a new age of technology and the ability to secure the technological and communications foundations of connected devices.

This issue brief is a collaboration between the Atlantic Council's Cyber Statecraft Initiative at the Brent Scowcroft Center on International Security and I Am The Cavalry.[3] It explores the opportunities that networked homes offer to society, along with the commensurate risks to security and privacy. It also offers recommendations for maximizing their value for homeowners while minimizing consumers' concerns, which may prevent or delay the smart home segment from achieving its market potential.

Smart Homes and Not-So-Smart Ideas

The notion of a smart home as the push-button solution to domestic drudgery was a staple of mid-century World's Fairs, Walt Disney, and *The Jetsons*. But it wasn't until the late 1980s that technology companies got on board, declaring "the house of the future" to be computing's next frontier. For the next twenty years, they pursued this vision, producing smart appliances of dubious value and at great expense.

Emblematic of these efforts is the Internet refrigerator, announced in 1999 (and finally introduced a decade later) as an all-in-one email, television, and personal finance terminal.[4] Contemporary versions start at $3,000 and have since added computer applications (apps), social media, and streaming music to the mix.[5] Consumers yawned; security experts flinched. The refrigerator's "new" features weren't compelling enough for consumers who already used other devices to access the same exact services. Security researchers were terrified of the risks another weakly secured, internet-connected device posed to consumers' security and privacy. Today, fewer than 5 percent of consumers have a smart refrigerator.[6] Despite nearly three decades of producers espousing the inevitability of smart homes, very few consumers have adopted their version of futuristic products.

A 2014 Acquity survey further underscores this point by juxtaposing its conclusion that "mainstream consumer adoption of IoT devices and technology is inevitable" with its result that 87 percent of consumers haven't heard of the term "Internet of Things."[7] How consumers will come to purchase products they've never heard of is an interesting paradox, highlighting the gap between the real and imagined popularity of connected devices.

It seems the key to adoption is to design and create products that add significant value to a consumer's life—and to do so cheaply. Health and fitness wearable technology is one specific product type that seems to hit the sweet spot between value-added function and affordability.[8] Additionally, a 2014 Deloitte Survey on mobile consumers (i.e., a population of early adopters of technology) reveals that 47 percent of US respondents found value in smart home solutions that allowed them to control lights, heating, and burglar alarms.[9] However, for some, a smart home just isn't in their future: 36 percent of consumers don't see the value in connected devices.[10]

> Consumer concern about hacking is the most serious barrier to adoption.

Consumer concern about hacking is the most serious barrier to adoption. Mobile consumers, when asked what the greatest potential issues were when using smart home technology, were most concerned about hacking, technology failure, and incorrectly set systems.[11]

3 A global volunteer initiative, focused on the intersection of public safety and cyber security.

4 "Making your kitchen cool," *BBC News*, February 10, 1999, http://news.bbc.co.uk/2/hi/science/nature/276870.stm.

5 Will Greenwald, "Samsung RF28HMELBSR/AA Refrigerator With Wi-Fi-Enabled LCD," *PC Magazine*, July, 22, 2014, http://www.pcmag.com/article2/0,2817,2460425,00.asp.

6 "The Internet of Things: The Future of Consumer Adoption," Acquity Group, 2014, http://quantifiedself.com/docs/acquitygroup-2014.pdf.

7 Ibid.

8 Ibid.

9 "The Internet of Things Moves In," Deloitte, 2014, http://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/internet-of-things-global-mobile-consumer-survey-infographic.html.

10 "The Internet of Things: The Future of Consumer Adoption," op. cit.

11 "2015 Global Mobile Consumer Survey: US Edition," Deloitte, 2015, http://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-global-mobile-executive-summary-2015.pdf.

Smart appliances like these may offer individual and society-wide benefits—but only if features are compelling and consumers see them as trustworthy. *Photo credit:* LG/Flickr.

In addition to looking for products that add specific and necessary value to their lives, most consumers would also consider buying connected devices and living in smart homes if it makes financial sense. In fact, consumers even appear willing to barter their privacy for additional savings. "Forty percent of consumers are willing to share data from their wearable devices with retailers or brands in exchange for coupons, discounts or information." By way of comparison, only 9 percent would do so without incentives.[12]

Smart home technologies can unlock both individual and society-wide benefits in different ways. They can provide financial savings, enhance convenience for consumers, contribute to more ecological and sustainable living, reinforce the buyer's sense of safety and security, and more. All of these benefits come alongside, rather than replacing, the enormous market potential (financial, product sales, development, etc.) that device makers and others are banking on.[13] But only if consumers believe that smart homes can deliver on the promises made by technology purveyors and futurists without unexpected side effects. The challenge for smart homes seems not a race for features, but to build trustworthy devices that reliably deliver the promised benefits; credible security is a big part of the solution to that problem.

The next section contains descriptions of three areas of smart home applications—home utility systems, home appliances, and home safety and security systems—along with the potential benefits and shortcomings of each. To put these benefits and shortcomings into perspective, a short, fictional narrative follows, which illustrates the unfulfilled promises and unintended consequences of a smart home if the technology goes astray.

12 "The Internet of Things: The Future of Consumer Adoption," op. cit.

13 Joao Lima, "Behold the 10 biggest IoT investments," *Computer Business Review*, April 9, 2015, http://www.cbronline.com/news/internet-of-things/behold-the-10-biggest-iot-investments-4549522.

Home Utility Systems

When Tesla Motors CEO Elon Musk unveiled the Powerwall last April, he presented the battery with the panache typical of a Silicon Valley smartphone launch, and it worked—within a week, Tesla had sold out of the $3,000 battery's entire first year of production.

Musk's timing was impeccable. Increasing efficiency and capacity have combined to reduce the costs of unsubsidized rooftop solar electricity down to between $0.13 and $0.23/kWh, well below retail prices in many global markets[14].

Clearly, Musk's notion of a smart home as one that intelligently regulates its own energy needs has resonance with consumers. Solar independence—and the considerable subsidies many governments have been willing to pay for it—has set utilities against strange new coalitions of environmentalists and libertarians, including Georgia's "Green Tea Coalition" aligning the state's Tea Party with the Sierra Club.[15] (This coalition successfully led an effort in 2013 to require Georgia's state utility company to purchase more electricity from solar providers, thus breaking up a large monopoly, and doing it in an environmentally friendly way.)[16]

In a related development, Google paid $3.2 billion the year before for Nest Labs, whose flagship smart thermostat doubled as a home electricity regulator and data collection device. It wasn't farfetched to imagine constructing an energy-efficient smart home around rooftop solar panels (perhaps from Musk's SolarCity startup), a Tesla Powerwall (and electric car), and a Nest thermostat to coordinate them.

Energy efficiency may be more important as an environmental impact than cost saving. Four of consumers' top choices for smart home and wearable device features in a McKinsey survey were energy-saving thermostats, connected lighting, auto-adjusting thermostats, and connected energy tracking.[17] However, consumers aren't simply interested in the expected cost savings from such products. In fact, only 38 percent of consumers choose to adopt smart utility products based on impact to their bill; the other 62 percent are driven by other factors, such as moderating user impact on the environment.[18]

BOX 1: ECONOMICS OF THE INTERNET OF THINGS

The IoT market thrums with new classes of devices not imagined before, driven by the latest, most compelling technologies. Getting those devices into consumers' hands quickly means shortening the development cycle to a minimum; Device makers who spend extra time testing, identifying flaws, and eliminating them are at a disadvantage.

In the United States, there is no software liability, so the costs of security failure fall to the buyer. Though many device makers are conscious of security concerns and want to do the right thing, investing in better security may not make sense from a monetary, cost-benefit standpoint. For device makers, the cost of reducing security risks may not outweigh the benefits from securing their products—especially if they are delayed to market. Furthermore, any incentive to invest in better security may be even smaller, considering that many of the potential security risks might never affect consumers. How much should a device maker spend when the costs of failure do not directly affect them?

Home Appliances

Smart home appliances are already available but have not seen the widespread adoption initially expected: As few as 1 percent of US consumers have a smart refrigerator, while a mere 5 percent of US consumers plan on getting one.[19] This trend isn't unique to the United States; consumers in Great Britain and Australia

14 "Deutsche Bank's 2015 solar outlook: accelerating investment and cost competitiveness," Deutsche Bank Responsibility, January 13, 2015, https://www.db.com/cr/en/concrete-deutsche-banks-2015-solar-outlook.htm.

15 Debbie Dooley, "A Tea Party leader explains why she's teaming up with the Sierra Club to push for solar power," *Grist*, August 12, 2013, http://grist.org/climate-energy/a-tea-party-leader-explains-why-shes-teaming-up-with-the-sierra-club-to-push-for-solar-power/.

16 Carl Lindemann and Jared Goyette, "The 'green' Tea Party fights for a more environmentally friendly GOP," *Public Radio International*, April 11, 2015, http://www.pri.org/stories/2015-04-11/green-tea-party-fights-more-environmentally-friendly-gop.

17 "Connected Home Survey," McKinsey & Company, 2015, http://www.mckinsey.com/spContent/connected_homes/pdf/McKinsey_Connectedhome.pdf.

18 "The New Energy Consumer: Architecting for the Future," Accenture, 2014, https://www.accenture.com/us-en/insight-new-energy-consumer-architecting-future.aspx.

19 "2015 ISACA IT Risk/Reward Barometer – US Consumer Results," ISACA, October 2015, http://www.isaca.org/SiteCollectionDocuments/2015-risk-reward-survey/2015-isaca-risk-reward-consumer-summary-us_res_eng_1015.pdf.

also demonstrate only a weak interest in having a smart refrigerator (2 percent of consumers in both countries) or in planning to have one (7 percent and 6 percent, respectively).[20] Mobile device customers—a highly connected group already—seem hesitant to adopt appliance monitoring on their apps—just 18 percent want this.[21]

Perhaps the biggest problem is that the features available on many of these smart home devices seem primitive compared to our expectations of the integration and convenience features common on mobile phones. The features don't tend to enable new and unique benefits, they merely replicate capabilities on one more screen. For instance, Samsung's top-of-the-line refrigerators can show Google Calendar in their displays, but they don't offer much benefit over combinations of existing devices. Though if smart products are designed properly and with consumer expectations in mind, consumers will buy.

A new generation of appliances will go beyond adding one more screen to our homes, and instead will augment or automate our decision-making. Smart sensors in these appliances generate information to be aggregated and correlated, such as the weight of milk cartons or egg containers in the refrigerator. This data can be fed into automation and integration systems that already know things about us, like our regular breakfast habits. These systems can subsequently help us make decisions—like giving us an estimate of the number of breakfasts we have remaining in our refrigerator while we're out at the store; or simply making the decision on our behalf by scheduling the next carton of milk or dozen eggs for delivery just before we run out. This next generation of smart appliances is already on the market, with devices like LG's refrigerator that can tell you how many beers you have left in the refrigerator from a smart phone app.[22] In December, Amazon received a patent on "anticipatory shipping,"[23] which allows the data it collects to feed automated decision-making systems.

A new generation of appliances will . . . augment or automate our decision-making.

This level of sophistication promises to change the way we live, freeing up our time and brain power for other things. The home of the future may integrate a Nest alarm clock with Google Calendar, Google Maps, and an autonomous, self-driving Googlemobile to maximize sleep and minimize your commute. The kitchen of the future may be one in which your smart coffee pot knows when to brew itself, your smart forks report whether your children have eaten sufficient breakfast (or too much), and your refrigerator is silently correlating your personal eating habits with your exercise history to balance your diet.

IoT for Home Safety and Security

In June 2014, Nest Labs (recently acquired by Google) acquired the startup Dropcam for $555 million, adding the company's namesake home security cameras to its portfolio. A year later, Nest re-launched its smoke detector, Protect. Combined with Nest's thermostat, as mentioned above, these products are promoted as more than the sum of their parts—in the advent of a fire, Protect would trigger the alarm, the rebranded Nest Cam would automatically begin recording, and the thermostat's motion sensors would detect if anyone remained in the home after evacuation.

Home safety and security are typically top preferences for consumers. For example, Canary, a technology start-up that develops easy-to-use home security products, raised a startling $2 million in a month on the crowdfunding site Indiegogo (its target had been $100,000) for its all-in-one home security system. In polls conducted by Deloitte and ISACA, approximately 40 percent of respondents valued[24] and planned to adopt[25] Home Monitoring technology.

20 Ibid.

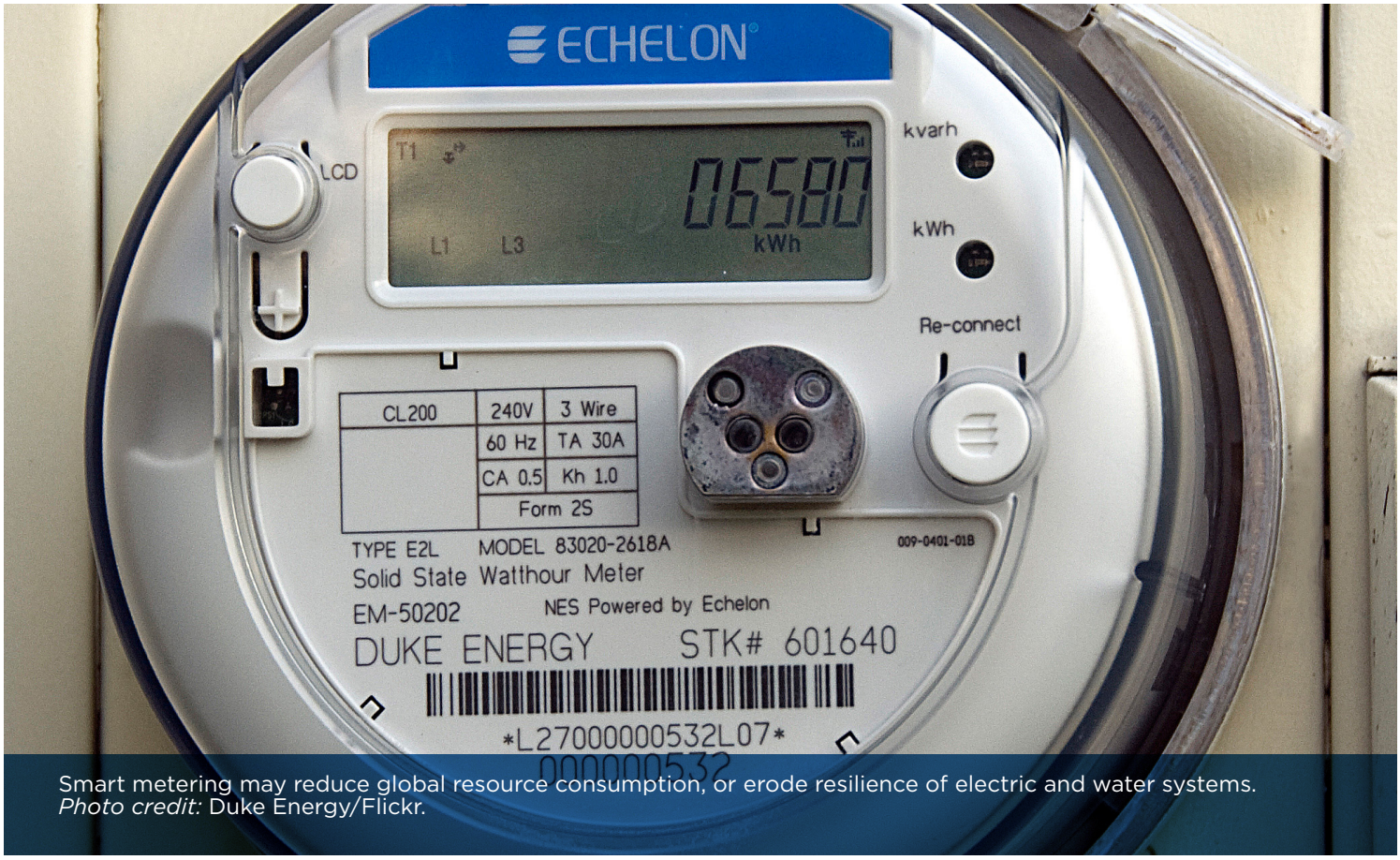
21 "The Internet of Things Moves In," op. cit.

22 Keith Wagstaff, "Out of Milk? LG's New Smart Fridge Will Let You Know," *NBC News*, May 7, 2014, http://www.nbcnews.com/tech/gift-guide/out-milk-lgs-new-smart-fridge-will-let-you-know-n99531.

23 Greg Bensinger, "Amazon Wants to Ship Your Package Before You Buy It," *Wall Street Journal*, January 17, 2014, http://blogs.wsj.com/digits/2014/01/17/amazon-wants-to-ship-your-package-before-you-buy-it/.

24 "The Internet of Things Moves In," op. cit.

25 "2015 ISACA IT Risk/Reward Barometer – US Consumer Results," op. cit.



Smart metering may reduce global resource consumption, or erode resilience of electric and water systems. *Photo credit:* Duke Energy/Flickr.

Haunting the Home of the Future

The future is never quite what you expect. Smart homes will only manage to reach their potential if the technology and value are right. Yet what are the potential consequences if things do not work out as planned? Paraphrasing Arthur C. Clarke's third law that "any sufficiently advanced technology is indistinguishable from magic," the interaction designer Tobias Revell offers: "Any sufficiently advanced hacking is indistinguishable from a haunting."[26] Without sufficient safeguards, smart homes could end up as haunted houses.

The brief, fictional narrative below explores themes of security, reliability, and business failures through a brief vignette set in 2025, when prevailing economic, political, and technological trends produce a hacked, "haunted" smart home. This narrative seeks to emphasize that the promise of smart homes must be backed by reliable technology decisions. In the absence of good choices, manufacturers risk the possibility that consumers will stop believing technology can positively contribute to society and change people's lives for the better. This scenario projects today's computer security risks into tomorrow's smart home, to illustrate a humorous worst-case scenario and illuminate many of the reasons consumers may choose to avoid smart home purchases.

Good Morning, 2025

For more than a month now, my house has been haunted. There's nothing supernatural about it; there are more than 15 million homes infected with the H@untedM@nsion worm, BuzzCNN reported yesterday. Every morning between 2 a.m. and 5 a.m.—never the same time twice—my bedroom lights begin to strobe, and Lou Reed's "Metal Machine Music" kicks in again. I would replace the smart lightbulbs (which were the

26 Tobias Revell, "Haunted Machines an Origin Story," July 26, 2015, http://blog.tobiasrevell.com/2015/07/haunted-machines-origin-story-long.html.

hackers' initial entry point into my smart home) with dumb ones, but then I'd lose the tax credits.[27]

Fortunately, I sleep on the floor of my Amazon Prime kitchen, which hasn't interacted with my Microsoft bedroom since the acquisition talks broke down in 2019. It's annoying when I ask for the weather report and both Alexa *and* Cortana talk over each other trying to answer. Even with my circadian rhythms shattered by the cacophony upstairs, Alexa knows me well enough to have started the coffee ten minutes ago.

I wish she had stocked the fridge with milk, however. I haven't had dairy in months, after hackers took advantage of my flirtation with the paleo diet to tweak Amazon's predictive ordering routine to have racks of lamb and other big-ticket meats delivered. They ship them to me through their referral code; this earns them pennies but costs me a lot more. If I give them away or throw them out, more arrive automatically. All I can do is let them rot in the fridge, pitting the algorithm's learning function against its zombie programming.

While the coffee brews, I take a shower. As part of the haunting, my security camera ritualistically snaps a photo while I'm *au naturel*.[28] When the haunting started, the first picture was accompanied by an automated email threatening to post my less-than-paleo physique to my Facebook account daily, unless I paid up–300 µBTC,[29] or about $20 US, to their bitcoin wallet.

There isn't sufficient power for me to work from home today. A 2022 Supreme Court decision granted power utilities the right to requisition stored electricity in my Tesla Powerwall during "periods of emergency" (i.e., summer), so by around noon I won't have enough power both to charge the car and run the smart lights. And I'll have to get back before 7 p.m., when the power normally comes back on. AT&T Cisco's Smart+ Connected Collection service has started refusing to unlock the door without a pro-rated daily payment to cover the utility bill. It's a good thing I never upgraded the door to the garage, so I can still hack its Bluetooth lock and sneak into my smart home.[30]

Maybe I'll just stay at Yuri's place again. As I access her smart fridge on my phone, I see not only what she has, but also what we need for a recipe it just found, based on how much we've liked the last few meals and from the health data recorded on our wearables. The app from the local seaport is showing a good harvest of Mackerel today, so her fridge sends my car the quickest route to the fish market, avoiding construction along the way. It's hard to leave the comforts of Yuri's place and go home, where I have the weather shouted at me while I eat meat for the rest of my life.

Environmental hazards from software and connectivity pose distinct challenges for smart homes.

Security Challenges

All systems can fail; there is no system without flaw. Engineers know this and adapt their work to be resilient against known and likely accidents and adversaries. Homes—smart or otherwise—are no different. But environmental hazards from software and connectivity pose distinct challenges for smart homes.

All software code has flaws and connectivity increases exposure of these flaws to more hazardous and potentially hostile interactions. A study by the Carnegie Melon Software Engineering Institute suggests that the lower limit for commercial software may be one to seven flaws per one thousand lines of software code.[31] However, the lines of code in each device continue to increase, as do the number of devices that constitute the systems of a smart home. The aggregate lines of code across all of our smart home devices are approaching hundreds or thousands of exposed, exploitable flaws if they do have not already surpass those levels. At

27 Smart bulbs are hackable, and can act as an entry point to your home network. Michael Armentrout, "Why Lightbulbs Will be Hacked," *EE Times*, September 29, 2015, http://www.eetimes.com/author.asp?section_id=36&doc_id=1327843.

28 Home security cameras were found to expose video feeds online, without owners' awareness. Tony Pipitone, "NBC 6 Investigation: Security Cameras Not So Secure," November 20, 2014, http://www.nbcmiami.com/investigations/NBC-6-Investigation-Security-Cameras-Not-So-Secure-283429931.html.

29 Micro-Bitcoin, abbreviated µBTC, represents 1/1,000,000 of a bitcoin.

30 Bluetooth door locks were found to be vulnerable to remote unlocking without owners' permission. Heather Kelly, "'Smart homes' are vulnerable, say hackers," *CNN*, August 2, 2013, http://edition.cnn.com/2013/08/02/tech/innovation/hackable-homes/.

31 Watts S. Humphrey, "Defective Software Works," *Software Engineering Institute, Carnegie Mellon University*, January 1, 2014, http://www.sei.cmu.edu/library/abstracts/news-at-sei/watts-new20041.cfm.

BOX 2: BAKED IN VS. BOLTED ON

Security that isn't "baked in" must be "bolted on" through additional devices and software, with costs borne by the consumer. Requirements built in from the beginning tend to be less costly and more effective than those bolted on later. Inherent, or "baked in," capabilities within a system reduce the number and potential impact of flaws because they are anticipated and integrated; bolted on capabilities are not. And, from experience with corporate IT, these bolted on security measures add cost, add complexity, require domain expertise, require monitoring, and fail regularly.[1]

Fortunately several initiatives are forming to help device makers build in security and preserve consumer confidence in the IoT space. I Am The Cavalry released frameworks to help automakers and healthcare stakeholders build safety capabilities into their product lifecycle: design, development, production, operation, maintenance, and retirement.[2] Other initiatives and organizations serve a similar function, such as BuildItSecurely,[3] the Online Trust Alliance,[4] the Online Web Application Security Project (OWASP),[5] the European Network Information Security Agency,[6] and the Institute of Electrical and Electronics Engineers (IEEE),[7] just to name a few.

1 "Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware," *Gartner*, August 22, 2014, http://www.gartner.com/newsroom/id/2828722; The number of data breaches from 2011-2015 is over 7,000 and growing. Open Security Foundation, "Data Loss Statistics." http://datalossdb.org/statistics.

2 "Five Star Automotive Cyber Safety Framework," I Am The Cavalry, August 2014, https://iamthecavalry.org/5star; I Am The Cavalry, "Hippocratic Oath for Connected Medical Devices," January 2016, https://iamthecavalry.org/oath

3 BuildItSecurly is a volunteer organization dedicated to building security capacity in kickstarter-sized projects, http://builditsecure.ly/.

4 The Online Trust Alliance, a non-profit organization focused on enhancing online trust, established a framework for IoT with principles based on privacy, security, and sustainability, https://otalliance.org/initiatives/internet-things.

5 The Online Web Application Security Project provides IoT testing guides, design principles, and other information to help individuals better understand the security issues associated with IoT, https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project.

6 The European Union Agency for Network and Information Security (ENISA) is the EU's lead agency for cybersecurity issues, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart-homes/security-resilience-good-practices.

7 The IEEE is the world's largest professional association for electrical and electronics engineers, http://iot.ieee.org/.

the point where this technology has the potential to impact human life and public safety, a higher level of care and attention is warranted.

Meeting the Security Challenges: Recommendations

IoT device makers can demonstrate to potential buyers their commitment to building trustworthy devices. These signals create a competitive advantage over products and brands that do not pay equal attention to safety and security. Integrating safety and security of the connected software components throughout the design and manufacturing phases aligns incentives, placing the cost where it can be most effective, and ensures a consistent customer experience that meets their expectations.

The following list includes many ideas already in practice for integrating security in design, as well as new ideas discussed among IoT stakeholders and identified here for more discussion.

- **Security by design** A published commitment to integrating security throughout the development, manufacturing, and deployment life cycle. Key elements, such as adversarial threat modeling,[32] resilience testing,[33] and reduced elective complexity,[34] lower costs and shorten the timeline of securing IoT devices.
- **Third party collaboration** A published policy accepting help from willing allies acting in good faith, such as customers and security researchers, who find and report flaws.

32 By anticipating hostile adversaries' motivations and behaviors, harm from malicious or malignant attacks against IoT devices can be reduced.

33 Testing systems for environmental hazards allows manufacturers to understand known failure conditions. In an Internet environment, adaptive adversaries and background hostility are some of these hazards.

34 Where a simpler solution will work, avoid using a complicated one. More lines of code, connectivity, and integrations create more inherent vulnerability and greater exposure to accidents and adversaries.

- **Failure investigation** Record and review evidence of failures to identify and address root causes, while preserving customer privacy.
- **Remote updates** A secure, prompt, and agile response to security or other flaws greatly reduces support costs, increases consistency of experience, and allows feature improvements over time.
- **Safe failure modes** Protections to ensure that failed or manipulated components do not put safety at risk. For instance, preventing the spread of failures, making failures evident, and failing in a way that does not harm safety or privacy.
- **Standalone Operation** Document which specific features and benefits will continue to work without Internet access and chronicle negative impacts from compromised devices or cloud-based systems. The most proactive companies may find it less expensive to buy back obsolete devices, rather than continue to support them.
- **Safe options and defaults** Give owners clear guidance on why and how to configure devices to their own particular preferences, and ensure that defaults are reasonably safe and secure.
- **Data protective measures** Describe the protection of customer data against unwanted modification, removal, or disclosure, including how to safely remove data upon resale, loss, or theft of the device (or home).
- **Informed consent for data use** Describe the ways in which customer data is used or will be used, as well as methods for consumers to opt out. This includes change in ownership of the company, or sharing information with third-parties.

Other good practices are emerging and will continue to develop over time as the smart home market matures. These recommendations are meant to work alongside, not to replace, practices already in place in the traditional manufacturing of consumer electronic goods.

All consumers—even non-technical ones—can use consumer protection remedies and market forces. The effect of consumers' actions can shape the decisions manufacturers make when bringing IoT devices to market.[35] However, their effects may take some time to manifest, as the design cycle can be months or years for new devices. Early adopters and those more comfortable with technology can employ more technical safeguards in the short term, such as changing default passwords, updating firmware, and reviewing security and privacy settings. Though buyers who tend to be less familiar with technology should not be inadvertently exposed to risk.

Conclusion

Smart homes have tremendous potential, especially when looking to the future of energy generation and consumption. Yet consumer confidence in many elements of the smart home is low, and safety and security risks appear to be increasing. It is time to be smart about designing and developing systems for smart homes. This is the difference between a future of comfortable interaction with home technology and a dystopian, haunted one.[36]

It is time to be smart about designing and developing systems for smart homes.

Smart homes in the Internet of Things can revolutionize energy generation and consumption, realize the 1960s dreams of home automation, and offer customers new capabilities for safety and security. But doing so will require a more proactive, preventative, and multi-stakeholder approach to IoT security challenges than that evinced by technology companies and policymakers to date. This paper has tried to frame the risks and benefits, culminating with a checklist of best practices for manufacturers and customers alike as they attempt to navigate a changing competitive and political landscape.

Much work remains to be done. As poll results indicate, consumer attitudes alternate between jaded and

35 For instance, the US Federal Trade Commission Complaint Assistant offers an online portal for consumers to report a variety of complaints. It is also possible to engage the retail channel to ask about protections against some of the common concerns outlined in this paper.

36 In the report *Risk Nexus: Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures,* the Atlantic Council's Brent Scowcroft Center on International Security, in collaboration with Zurich Insurance Group and University of Denver's Pardee Center on International Futures examines alternate cyber futures and their impact on global economic growth, innovation, and prosperity.

excited, or scared, and with good reason. Buyers and manufacturers need to be resourceful about selecting, constructing, and securing smart homes, lest one day poltergeists haunt the residences.

Greg Lindsay is Nonresident Senior Fellow at the Atlantic Council's Strategic Foresight Initiative, Senior Fellow at the New Cities Foundation, visiting scholar at New York University's Rudin Center for Transportation Policy & Management, contributing writer for Fast Company, and co-author of *Aerotropolis: The Way We'll Live Next*.

Beau Woods is Deputy Director of the Cyber Statecraft Initiative at the Brent Scowcroft on International Security, where he focuses on the intersection of cyber security and the human condition, primarily around cyber safety. He also works closely with the I Am The Cavalry civil society initiative, ensuring the connected technology that can impact life and safety is worthy of our trust.

Joshua Corman is Chief Technology Officer for Sonatype. A respected innovator, he cofounded Rugged Software and I Am The Cavalry to promote new security approaches in response to the world's increasing dependence on digital infrastructure. His unique approach to security in the context of human factors, adversary motivations, and social impact has helped position him as one of the most trusted names in security.

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org