Research Note

Smart Homes: Evaluating Risks and Being Smart in the SmartHome Revolution

Mikhail Savvateev

September 2017

Keywords: Smart Homes; Internet of Things;

Abstract: This paper discusses the emerging risks associated with the "Smart Home" technological advances that are becoming increasingly ubiquitous across the human experience. "Smart Home" is the term commonly used to define a residence that has appliances, lighting, thermostats, electronics, and other systems that are capable of communicating with one another and can be controlled remotely via the Internet. The author examines how these new technologies have created new security and other technological system risks, and provides some suggestions for industry participants.

Introduction

The Smart Home revolution, which has recently been gaining momentum in the markets, is the first major change in decades affecting how we live and interact with our dwellings. Because of this movement, many novel technologies will finally make it into the average household, and the next several years will show both the benefits and potential dangers of this shift. A new and rapidly growing market of this kind is prone to many internal and external risks, and it is imperative that the industry's key players and up-and-comers alike consider these risks, ensuring the market and the innovations it inspires reach their full potential.

Background

Smart Home technology is the household application of the Internet of Things (IoT), which is a major technical trend spanning many industries worldwide. The IoT is the principle of giving devices connectivity capabilities. This allows devices to form networks which record, process, and share data in order to improve their utility and optimize their operation, linking them together for coordinated execution. Ultimately, by linking the functionalities and data streams of multiple devices, and tapping into processing capabilities (which can be located remotely or within one of these devices), the goal of the technology is to learn about people's habits, and adapting how each device functions in order to meet each user's unique needs.[1] This means that in the future, Smart Home solutions might be able to automate complex tasks involving learning and predicting customers' preferences, such as controlling house heating or cooling systems to maintain optimal temperatures while saving power, or taking care of pets in accordance with the animals' preferences and habits. As a result, we could reach what might be considered the ultimate level of convenience, since household tasks will be handled automatically without needing the user to program instructions, operate triggers, or even think about the task being done.

The Market

Though consumers are some time away from being able to purchase fully automated homes, there is already a lot of

excitement surrounding devices and appliances with networking capabilities. A 2015 report by Icontrol Networks, a leading Smart Home developer, cites a global study by the Gartner research company showing that 50 percent of consumers planned to purchase a connected device within a year.[2] Analysts expect sharp growth across the industry, predicting that in contrast to the 15 billion IoT devices active worldwide in 2015, by 2020 there could be as many as 200 billion devices across the globe.[3] Gartner expects that by 2022, a typical family house could contain over 500 smart devices.[4] While the exact magnitude of growth is difficult to predict, these figures paint a very optimistic future for the sector and tell us of the massive potential in Smart Home development.

Not only are these devices very prevalent and continuing to spread, but they also touch on nearly every aspect of the modern home. Market research shows that the most common reasons given for purchasing household smart devices are: home security, cost-saving potential, convenience, environmental friendliness, productivity, entertainment system enhancement, and access to advanced communication functionality.[5] These span nearly everything relating to one's house, and as time goes on, more and more devices and systems will crop up seeking to fill these needs. From existing products like connected thermostats, light systems, and cameras, to futuristic systems like independent cooking or cleaning automatons, soon these devices will control every element of the home.

While the possibilities presented by this sector are exciting for both consumers and businesses, the staggering magnitude of these devices' spread, pervasiveness, and variability drives home the point of how important it is to ensure that the companies behind these devices do everything to mitigate any relevant risks. Possible pitfalls and dangers surround every young technology, and failure to manage them can have huge repercussions as that technology develops. At this scale, even seemingly minor issues and risks can be catastrophic for businesses and whole segments of the market. Therefore, as excitement surrounding Smart Homes persists, the only way ahead is to avoid potential risk and to ensure proper measures are in place at every step of the technology's development.

The Sector

Smart Home technologies, and the Internet of Things as a whole, have evolved very rapidly in recent years. As such, the producers' market remains largely decentralized: examination of popular products and lists of market leaders reveals that major players are a mixture of companies of many different sizes and focuses.[6] While large tech firms (e.g. Google, Amazon, GE, etc.) are starting to invest in and consolidate Smart Home solutions, many winning products continue to come from startups or small companies focused solely on IoT device production. Smart lighting is a good example: network-connected lights are set to generate global revenue of roughly 17 billion dollars in 2016, which is distributed across brands that vary greatly in size.[7] Leaders come from giants in the standard lighting market like GE and Philips, as well as segment-specific startups such as LiFi, whose LIFX bulbs are very popular with American consumers even though the company is a newcomer on the tech scene with humble beginnings coming out of a 2013-2014 Kickstarter crowdfunding campaign.[8] Therefore, the industry also has to deal with mass decentralization while trying to tackle the aforementioned boom in demand. On one side, the prospect that any company can participate is good for innovation and controlling prices, however, when considering how to ensure these eclectic networks of devices are compatible and secure, the lack of clear leaders in the market makes piloting solutions or industry standards an arduous procedure at best. This of course further complicates the business' abilities to manage risk and react to problems, making early risk analysis all the more crucial.

Risk Analysis

The Smart Home concept, like any novel field, has its fair share of risks. New technologies being pioneered often create security and other technological system risks, while the initial dive by companies big and small to seize a slice of the fresh market often breeds process risks as this high-urgency development tends to leave any talk of procedures or standards in the dust. Finally, no market boom goes unnoticed from the outside, and external risks spring up as everyone from criminals to government actors attempt to either exploit or control the young industry for their own

needs. It is important to investigate these risks in depth, as failure to resolve them can kill a growing new sector as fast as it was created in the first place.

System Risks

As was demonstrated in the discussion of Smart Homes' market, the industry as it stands must deal with a largely disjointed set of products. Because of being such a decentralized market with a very strong startup presence, a consumer today will likely purchase every element of a Smart Home system from a different manufacturer. Combined with a lack of industry standards, this leads to a dismal state of security and standardization across the board.

Disjointed Connection Procedures

A major source of problems as Smart Homes evolve is the fact that the industry has not created a universal standard for connections. Different devices use a variety of protocols and technologies, such as Bluetooth, Wi-Fi, RFID, and others, to form connections and transmit data. Issues arise when mismatches in these technologies create either connection problems for customers, or worse, create security gaps which can make systems vulnerable to attack.[9]

If companies do not take care to select the right connection methods, it is quite apparent that customers may run into either connectivity problems, or interference if different devices attempt to use the same channels, or wavelengths to simultaneously send information. For example, RFID tags are cheap, low-energy connectivity chips that allow data transfer between nearby devices, and work through a setup of readers and tags able to transmit signals. They are often used in IoT due to their low cost and energy efficiency. While these chips are undoubtedly useful, they fall short on many of the factors needed for sound Smart Home system design. For example, RFID readers are not very good at handling multiple connections, so a lot of work must go into collision resolution fail-safes, which prevent malfunctions if several tags contact one reader at the same time.[10] Because there are no established guidelines for designating uses for the range of RFID tag signals, companies have much more difficulty and must dedicate additional resources to developing anti-collision algorithms. If a logical system was in place for assigning ranges of RFID frequencies, filtering out extraneous signals would be much simpler, and consumers would be safer from technical failures resulting from programming oversights or coincidental frequency collisions.[11] This correctable oversight is a possible source of reputation and financial risk for manufacturers (since regular technical issues will lead to a poor customer experience, an image of a buggy product, and ultimately loss of sales), and there is even potential legal risk if inadvertent signal collisions cause damage or injury through the failure of vital systems like health monitors or home security devices. These problems are present (to varying extents) in all connectivity protocols which are in use today, so it is certainly a considerable risk all IoT manufacturers must deal with.

Additionally, experts predict that soon many of the current connectivity technologies will face the problem of bandwidth oversaturation. In the last few years, network traffic has grown considerably, and with IoT development leading in a new influx of connected devices, continuity will be a growing problem as time goes on.[12] Unless new tech is introduced to expand the available bandwidth range, providing all devices access to the data streams that they need will be more and more difficult. Even if local collisions (like those common with RFID devices) are avoided, increasingly large and bandwidth-hungry systems will have to learn to share progressively more crowded networks. If congestion on networks becomes too extreme, customers may start to ditch IoT in favor of higher-priority Internet use. To avoid being labeled an industry of network vampires capable of slowing users' connections to a snail's pace, Smart Home companies must work together to find a solution.

In general, connectivity options are not a main consideration in device design, typically playing into other questions like hardware costs. But to avoid pushing home networking into a state of battle over resources and forcing consumers to choose which of their devices are most deserving of a connection, IoT manufacturers must work together to optimize their bandwidth use and protocol selection. As convenient as connected Smart technologies are,

most consumers will not sacrifice internet speeds or the smooth operation of vital systems (e.g. health monitors) for some added comforts.

Vulnerabilities and Security Issues

Security and privacy worries are at the forefront of the concerns people have about the Smart Home sector. The Smart Home movement is seeking to place an unprecedented number of network-connected devices capable of data collection and given control over physical processes in consumers' homes—a traditionally private and intimate place for most people. So, there is no surprise that fears of breaches prevail, even among early adopters.[13] High profile cases bringing up the possibility of IoT hacking, such as the 2015 experiment where researchers were able to access internet-connected baby monitor feeds[14] often make rounds in the news and heighten consumer fears of the technology. New markets are especially sensitive to sector-wide reputation risks as mass fear over the new tech can seriously harm sales and set back pioneering firms. On top of this, financial and legal risks can be a considerable problem for companies if a breach is to occur and customers seek damages for failure to protect their data.

There is a number of security-related oversights in how most Smart Home systems are designed, and it is an unfortunate reality that such new and rapidly-growing markets tend to lead to a culture of brushing off best practices (most notably in security) in a rush to release products sooner. In a recent survey by online authentication provider Auth0, 85 percent of IoT developers admitted to being pressured to get a product to market even though the implementation of adequate security software was not yet completed. This abysmal statistic shows how critical (but fixable) the problem is, and outlines a prisoner's dilemma for the Smart-Home sector: unless all the market participants put their competitive drives on hold and focus their attentions on dealing with these issues and rectifying their security-averse practices, soon enough there might not be a market to compete over.

Studies point out some of the most severe problems with the way security is implemented in IoT devices today. A very serious one is the lack of connection protocols. Going back to the RFID example from earlier, consider that RFID tags have very low processing capabilities and thus can only use lightweight authentication solutions, which can be less secure. As there are no established industry-wide standards, devices that can tolerate the risks of low-strength authentication are able to connect to high-risk devices such as medical equipment, thus exposing the more vital machine to unauthorized access. Another problem is the deficiency of encryption in communication between devices, with some devices even failing to encrypt key data like passwords or security certificates[15]. While encryption can be hard to maintain when working with embedded devices not powerful enough to run standard encryption algorithms,[16] consumers' focus on the security and privacy warrants favoring secure solutions over more lightweight or energy-efficient ones. Unencrypted information is easy to intercept from a network, so it is imperative IoT device makers follow basic procedure for their own data, and respect the security of information received from other systems. Other issues, such as the lack of password strength rules or account-locking defenses (to fend off automated attacks) are reported to be just as prevalent. There is also a surprising lack of support for functionality for the manufacturer to be able to remotely send out firmware updates or patches to devices as a way to resolve security problems.[17] HP ran a study last year on ten popular IoT security systems, and found rampant failure to either properly configure or even to attempt to implement minimal security basics like encryption, proper authentication, or the capacity for remote updates. A hundred percent of the tested devices failed at least one basic check.[18]

Following initial IoT trends, Smart Home developers tend to focus on low-power systems, minimal local processing, and the simplest overall solutions in order to reduce cost and energy consumption of devices. This is now a big concern for the industry: to earn consumers' trust and lay a framework for future growth, some of the current minimalism must be traded in for stronger security before consumers are scared off for good.

Process Risk

As was briefly mentioned in the discussion of Smart Home security risks, part of the problem with IoT today is that

industry-wide oversight and coordination on security and privacy issues is largely absent. Not only does this make it harder to maintain a secure system when multiple products and manufacturers are involved, but it leaves a control vacuum which—in the case of a major breach or public outcry—might lead to increased government regulation. However, government regulation may either solve some of the security issues or hamper furutre innovation with overcomplicated policies and burdensome auditing procedures.[19]

Lack of Consumer Education Initiatives

A common sentiment in the computational security industry is that the biggest vulnerability is the user. After all, the strongest password encryption methodologies are powerless if the user leaves the password on a sticky note by the keyboard. Therefore, vendors of Smart Home systems should ensure customers are instructed and guided to make sure that the defenses that are in place on their devices are being utilized fully.

A key example is relating to the use of default passwords on connected devices. When purchasing an internet-connected device, customers are typically given a default username and password, which they are theoretically expected to change during setup. This is often not the case, which largely defeats the purpose of a password. There already exist copious online databases listing varying IoT devices and their default login information, meaning hackers trying to access a device can automatically try the default information with little difficulty.[20] The magnitude of the problem is exhibited in the Dyn cyberattack of October 2016. The hackers involved built a bot network by compromising IoT devices worldwide, and used them in a massive DDoS attack. When the code used in the attack was examined, security analysts found that the botnet, which at its peak was made up of roughly 400,000 devices, was created by simply attempting to use a list of 61 passwords on each encountered device. Therefore, hackers could harness almost half a million devices by trying a few dozen passwords (many of which were standard defaults like "admin" and "root").[21] If the owners of these devices were given a few pointers on the creation of strong passwords, and perhaps guided with simple authentication system enhancements such as password strength or double authentication requirements and the implementation of one-time first-use credentials,[22] Dyn Inc. would not be looking at the aftermath of the biggest DDoS attack recorded in history.[23]

Absence of Industry Standards

Also tying closely to system risk is the industry's failure to formulate any kind of standards or best-practices to date. Unless the industry forms some sort of accepted protocol to be used across the Smart Home market, manufacturers will continue to face connectivity, compatibility, and security risks. There will be immediate benefits from industry-wide oversight, which will greatly reduce the third-party risk of a company allowing a connection to any other manufacturer's devices.

Due to their interconnectivity, Smart-Home Systems follow the principle that "a chain is only as strong as the weakest link," so the breaching of any element can allow a lithe hacker to access any other part of the network. For instance, while the manufacturer of a smart toaster oven might have little concern for security (what sensitive data can be stolen from a toaster?), if that toaster is hooked up to the same network as important devices containing sensitive data, suddenly that toaster is a liability. This can hurt both the toaster's manufacturer for being at fault for the penetration, as well as the company behind the more sensitive devices for failure to prevent the attack. Therefore, it is in the interest of every developer of Smart Home technology to ensure that they and the other players in the sector follow the same security procedures.

External Risk

Hacking and Loss of Privacy

The issue of the possibility of malicious or unwanted access to IoT devices and data in the home is a repeating theme in examining possible risks within the industry, and likely poses the gravest threat to Smart Home sales.

Privacy concerns are especially big among potential consumers, given how much the technology can be embedded in every element of the home. With this massive capacity for generating data, consumers worry about the disclosure of information ranging from embarrassing (such as fitness tracking weight data) all the way to highly important and personal, like "the user's residence location, income, lifestyle, behaviors, heath status and other sensitive information."[24] At that, users are concerned about different levels of data leakage, from malevolent, forced entry by hackers, to unwanted data collection by companies for marketing and research, all the way to fears of government surveillance. As put by the *Wall Street Daily*, "without privacy assurances, wide-scale consumer adoption simply won't happen."[25]

Additionally, the hijacking of devices by hackers for use in major cyber-attacks is a growing concern. Even though, according to chief research officer of F-Secure Mikko Hypponen, consumers mostly do not care about their devices' possible involvement in cybercrimes (especially if the operation of the device is unaffected),[26] other risks will affect the industry if the threat is not dealt with. Due to the sheer scale and spread of the IoT device market, botnets targeting these devices can quickly acquire thousands of nodes, which form a formidable threat to any server or network they are used to target. Like the aforementioned Dyn hack, which utilized almost half a million IoT devices to take down a major DNS server and thus forced several major websites offline in parts of the US for several hours, this vulnerability poses a massive threat which is very hard to combat due to the decentralized and complex nature of such cyber-attacks.[27]

Attacks of this scale can cause huge finance losses, physical infrastructure damage, or even loss of life if certain vital utilities or centers are targeted. As a result, failure to react to these threats results in a big risk of government involvement in the industry, which can hurt startups, increase manufacturing costs, and in general bog down any drive for innovation with audits, checks, and bureaucratic procedures.[28] This would especially threaten IoT manufacturers in countries that do implement government control, since delays and costs induced by regulation can give the advantage to regulation-free foreign firms, all while failing to do much about the problem if international manufacturers do not need to comply with these rules and their products remain vulnerable.[29] Even with these downsides to regulating the sector, the government may feel its hand forced in light some major incident, so proactivity is key to preserving the industry's freedom.

Reputation

Another repeating theme that ties to a number of the other risks is the impact certain problems can have on the reputation of IoT technology, which can directly affect sales. As the industry stands on the cusp of being able to offer full Smart Home solutions that cover all elements of the household to the average consumer, a make-or-break element is how people feel about the technology. The media has been happy to publicize breaches and research into security problems in popular devices, so even a single major event can turn off the masses to the idea of IoT-powered homes.

Customers' (often well-justified) concerns with privacy and security are major barriers to adoption of the technology, with a survey run by Auth0 showing that 52 percent of consumers and a shocking 90 percent of developers do not feel that IoT is secure enough.[30] So as was stated above, unless the industry comes together to handle these problems and invests in marketing to reassure buyers, the initial excitement over the potential of Smart Homes can sizzle out, forcing IoT tech vendors back to peddling their wares in fringe markets.

Mitigation

As Smart Homes have not been a part of mainstream markets very long, their sector seems surrounded by threats, and the prospect of having to counter them all is daunting even to already-established tech companies, and can be downright terrifying to startups. So how can the industry retain its youthful vigor and vibrant startup and

innovation scene while resolving the risks that look to be forming an existential threat to the whole market?

The ray of light in the darkness might be the collaborative environment in the hi-tech sector. If competing Smart Home companies can come together (as they already do to some extent in allowing their devices to interface with other companies'), they can cooperatively resolve the above risks and help their market grow into a much more stable and expansive segment of the technology and household appliance sectors. Here are some major recommendations:

Industry Consortium

An organization of sector leaders and major players is a key first step to resolving much of the industry's fragmented nature. By working together, companies can come up with standards for technologies used, connection and transfer protocols, and security requirements. This will resolve the major system and process risks faced by each company thus saving time, simplifying development, and ensuring consumes get the best experience. Additionally, this will mitigate reputation and legal risks across the sector since the consortium can guarantee products that it produces are compliant and secure, thus upping the security level across the industry and reassuring consumers in a highly visible and easily marketable way. Plus, the formation of an institution where industry stakeholders can resolve common issues can improve response rates to threats and breaches, helping enterprises of all sizes to respond to new vulnerabilities, counter ongoing crises, and recover from any incidents. Finally, an established collective of key market players will be a better platform to negotiate with governments and simplify the discussion of any reform or action as needed, as well as a unified channel for communicating with the media and other organizations. Augmenting the companies' outreach abilities is a good way to improve consumer relations and build trust as well, further buffering the industry from reputation risk.

Security Improvements

Each company in the Smart Home market should also take individual steps to strengthen their security protocols, perhaps with enforcement from the aforementioned consortium where needed. Relatively simple steps like implementing improved and expanded encryption, enforcing strong passwords and multi-step authentication, adding the framework for rapid firmware and security update deployment, and strengthening the security and general architecture of digital user interfaces do not add too much bulk to IoT devices or require much work. These are all common practices in other branches of software development, but can make a huge difference in improving device security.[31] Even something as seemingly trivial as forcing a password reset when setting up a device can help prevent massive breaches like the Dyn hack.

In general, companies should maintain a focus on eliminating vulnerabilities and following best practices during development of their hardware and programs. This approach is taken in much of the software industry, and helps ensure that the system is as impenetrable as possible. This cannot be done if security is added as an afterthought. While there are other drivers, like the desire for energy-efficiency, each manufacturer and the industry as a whole will benefit from secure design that and If these principles are outlined and accepted by an association of sector players, companies will be assured of their partners' compliance, and thus will have an easier time in development since they can focus on external threats, without having to worry about vulnerabilities within the system.

Changes in Approach

If the industry lags in adopting the two previous recommendations, a few major players might take the initiative and redirect the market to otherwise resolve the market's problems.

The Full Package

One possible direction for the market is a large corporation developing a single packaged solution for the Smart Home. With one manufacturer making all of the components, there will be no concern for compatibility. Security

risks can be dealt with by building safeguards throughout the system, and since one company manages the whole system and has full control of its peripheries, security can be further improved by surrounding the system with a single firewall. Again, problems with standards, protocols, and resource sharing will be made irrelevant by the single company's full authority over the system.

This grab-and-go solution, though likely more expensive and coming at the cost of customizability, will make Smart Homes quicker to establish since consumers pick a package as opposed to selecting individual devices. The full control and security focus will also make accessing the market much tougher for small companies; the resources needed to put together a wholesome, pre-packaged system exceeds those available to startups, and a large corporation managing such an ecosystem will certainly make it difficult to access its systems and integrate any third-party devices. Almost like the Apple Inc. approach to Smart Homes, this solution has a number of tradeoffs, and though a major win for the one or two enterprises that manage to push it into the mainstream, it will be a huge blow to the innovation of the technology and the freedom of the market as a whole.

The Control Center

Another possibility is a more liberal version of the above where a corporation creates a central hub to which a user can connect other devices. This corporation essentially takes on the role of an industry consortium, and will have to vet third-party manufacturers and enforce certain levels of security and mutual rules in order to overcome the general sector's problems. Potentially, these hubs can become much more secure by changing to an intranet configuration and doing all processing locally, without the need for external Internet connectivity. Of course, closing the system to all outside connection will make it much more secure. Though a little less monopolistic, this approach also places a lot of power in the hands of one-two market leaders and complicates the process for new devices to get to the market. Though a sound solution, the optimal route is of course a more free-market-based approach.

Conclusion

Today, there is a lot of excitement around the application of the Internet of Things within the home. The collective human fantasy has long run wild with images of automated houses that take the effort out of household maintenance and provide its residents with a multitude of benefits in every category of home living. Being a staple of science fiction works for many decades, Smart Homes have at some point entered the daydreams of almost every person, painting tantalizing pictures of delicious meals ready at the click of a button, chores taken care of with a wave of the hand, and every whim fulfilled with but a flicker of thought. Now, for the first time ever, one does not need to be a king or sultan to command such powers. With a few purchases, any household task can be bent to one's will.

However, in this age of constant security fears and technological growth, customers cannot be kept with just offerings of neat shortcuts and household optimizations. Customers will not give up privacy, risk security breaches, or compromise the functionality of their other gadgets just to say they live in a "smart" home. Therefore, every player seeking to capitalize on the opportunities the Smart Home market entails must think about sustaining the interest and enthusiasm amongst consumers with truly beneficial products oriented towards meeting all of the purchasers' needs. If the products end up causing users more headaches than they resolve, the market's excitement will quickly fade into nothing more than a passing fancy.

As difficult as it is to put aside competitiveness in such a fresh, ripe market, the best chance businesses entering this sector have to ensure their developments persist and avoid becoming a dying fad is a collaborative approach to solving the primary problems facing the industry. By taking steps that seems counter-intuitive in a free market and putting off the instant gratifications of cashing in on quick product releases, the Smart Home sector can ensure it has a bright, fruitful future and will see its key players usher in a future where fully automated Smart Homes pass from humanity's reveries into every household's reality.

[1] "Technology Driving Innovation - The Internet of Things: The Next Mega-Trend." Goldman Sachs. N.D. Accessed 07 Dec. 2016 <www.goldmansachs.com>.

[2] "2015 State of the Smart Home Report." Icontrol Networks. Jun. 2015. Accessed 07 Dec. 2016 <www.icontrol.com>

[3] "A Guide to the Internet of Things Infographic." Intel. N.D. Accessed 07 Dec. 2016 <www.intel.com>.

[4] "2015 State of the Smart Home Report."

[5] Ibid.

[6] "Top 50 Home Automation Companies." Home Automation Info. N.D. Accessed 07 Dec. 2016 <www.homeautomationinfo.com>

[7] Smallwood, Philip. "Lighting, LEDs and Smart Lighting Market Overview." U.S. Department of Energy. Feb. 2016. Accessed 07 Dec. 2016 <www.energy.gov>

[8] Schroeder, Stan. "Smartphone-Controlled Light Bulb Raises $260,000 on Kickstarter." *Mashable*. 17 Sept. 2012. Accessed 07 Dec. 2016 <www.mashable.com>.

[9] Jing, Qi, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qui. "Security of the Internet of Things: Perspectives and Challenges." SemanticScholar. Springer Science Business Media. 17 June 2014. Accessed 07 Dec. 2016 <www.pdfs.semanticscholar.org>.

[10] Ibid.

[11] Ibid.

[12] Kumar, Ajay. "Internet of Things (IOT): Seven Enterprise Risks to Consider." *TechTarget*, Mar. 2014. Accessed 07 Dec. 2016 <www.internetofthingsagenda.techtarget.com>.

[13] Prince, Brian. "Consumers Ready for Internet of Things, But Fear Data Privacy and Security Implications: Survey." *SecurityWeek*. 23 Jun. 2014. Accessed 07 Dec. 2016 <www.securityweek.com>.

[14] Stanislav, Mark, and Tod Beardsley. "Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities." Rapid7. Sep. 2015. Accessed 07 Dec. 2016 <www.rapid7.com>.

[15] Storm, Darlene. "Of 10 IoT-connected Home Security Systems Tested, 100% Are Security Failures." *Computerworld*. 11 Feb. 2015. Accessed 07 Dec. 2016 <www.computerworld.com>.

[16] Jing, Qi.

[17] Storm, Darlene.

[18] Ibid.

[19] Weiner, Jonathan B. "The Regulation of Technology, and the Technology of Regulation." Duke University School of Law. 2004. Accessed 07 Dec. 2016 <www.scholarship.law.duke.edu>.

[20] Reidel, Daniel. "IoT Default Passwords: Just Don't Do It." Dark Reading. 13 Oct. 2016. Accessed 07 Dec. 2016 <www.darkreading.com>.

[21] Ragan, Steve. "Here Are the 61 Passwords That Powered the Mirai IoT Botnet." *CSO Online*. 03 Oct. 2016. Accessed 07 Dec. 2016 <www.csoonline.com>

[22] Reidel, Daniel.

[23] Ragan, Steve.

[24] Jing, Qi.

[25] Basenese, Louis. "Internet of Things: Five Barriers to Adoption." *Wall Street Daily*. 21 Dec. 2015. Accessed 07 Dec. 2016 <www.wallstreetdaily.com>.

[26] Price, Rob. "The Government Needs to Step in and save the Internet from Hacked Toasters." *Business Insider*. 25 Oct. 2016. Accessed 07 Dec. 2016 <www.businessinsider.com>.

[27] Ibid.

[28] Weiner, Jonathan B.

[29] Price, Rob.

[30] Basenese, Louis.

[31] Roe, David. "Top 5 Internet of Things Security Concerns." *CMS Wire*. 30 July 2014. Accessed 07 Dec. 2016 <www.cmswire.com>.