ETHICAL IMPLICATIONS OF THE INTERNET OF THINGS

Matthew S. Levan
mlevan1@toromail.csudh.edu
Computer Science Department
California State University, Dominguez Hills

Abstract

The Internet of Things (IoT) promises to improve modern life via enhancing everyday objects (cars, home appliances, wearable devices, phones, etc.) with embedded electronics, software, sensors, and Internet connectivity. To provide users with more services than the devices alone could provide, the IoT relies on communication—relaying data between manufacturers, operators, and/or other connected devices via the Internet[1]— but, while the benefits of such functionality are widely marketed and promoted, the security of the IoT is often overlooked and, at worst, even neglected. Therefore, dedicating as many resources to IoT security as to IoT features has become of utmost ethical importance and, accordingly, such ethical conduct in the development and maintenance of IoT systems and products is essential to professional success in today's voraciously competitive technology marketplaces. This paper will provide background information on computer ethics and the IoT, examples of known IoT exploits and security vulnerabilities (for both safety and privacy), and explore the ethical implications of IoT vulnerabilities.

Keywords: Internet of Things, Security, Safety, Privacy, Ethics, Computer Ethics.

1. INTRODUCTION

Technology continues to rapidly change the modern world in which we live. Computers are ubiquitous even in less affluent nations as the "mobile revolution" continues to sweep the globe. As Moore's Law continues to hold true, electronic hardware like computer components (CPUs, GPUs, RAM, digital storage devices, systems on a chip, etc.) and on-board sensors (health-related tracking, accelerometers, gyroscopes, temperature, image, etc.) continue to become less expensive, more powerful, and smaller in physical size. Access to broadband Internet connection is fairly ubiquitous, although data transfer speeds have quite a bit of room for improvement.

With these leaps in the evolution, as well as mass adoption, of technologies serving as a sturdy foundation, the Internet of Things (IoT) was born. At its best, the IoT is a compelling new paradigm in technology that aims to provide new services, greater effectiveness and efficiency, and convenience by creating networks of Internet-connected devices or "things" and utilizing each thing's corresponding capabilities. However, due to the "influence of several contributing trends, as well as various interpretations of the phrase in everything from scientific research to marketing materials," the exact definition of the "Internet of Things" is debated[2]. For the purposes of analyzing the ethical implications of security vulnerabilities in the IoT, let the phrase strictly refer to the ubiquitous network-connected technologies and the data produced and consumed by those technologies.

Because of the nature of IoT objects and technologies being increasingly immediate and directly influential in one's environment (think medical devices instead of computer desktops), physical safety is also a concern. As promising as the IoT already may be, the fact that the IoT leverages these types of objects that are potentially dangerous in people's lives (cars, stoves, refrigerators, etc. rather than simply a laptop or desktop computer), concerns regarding the safety of the IoT are quite justified. Security vulnerabilities in the IoT can be *physical* while vulnerabilities in traditional computers are *digital*. Disasters due to malfunction and/or hacking are a very real concern.

Of course, inadequate security in IoT technologies means potential threats to physical safety as well as threats to user privacy. The ACLU has expressed deep concern with regards to the IoT's potential for degrading people's privacy and control of objects in their lives by arguing that, with Big Data and the IoT combined, powerful corporations and governments will essentially be able to extract any and all information from user's lives at will[3]. Since most, if not all, of the benefits of the IoT arise out of the ability of IoT technologies to intelligently control systems (via data collected and shared by the devices within an IoT system) without human interaction, there is an inherently greater amount of private data available to be leaked to the prying eyes of governments, corporations, or hackers. While physical safety is of top concern to an ethical IoT professional, user data privacy is not trailing far behind.

For reasons of safety and privacy, any ethical professional who is responsible for the production, deployment, and/or technical maintenance of IoT technology should treat product security at least as seriously as product features, if not more so. Intelligent strategies for ethical conduct in the IoT business, and especially the business of *securing* IoT products and services, are of utmost importance for success and longevity in the competitive technology market.

However, even systems and products created with the heaviest attention to security are *never* completely secure. On that same vein, if a hacker manages to attain elevated access to the software in someone's smart toaster and successfully manipulates the heating element enough to start an electrical fire, who is responsible? Are brands and manufacturers ethically responsible for each and every exploitable security vulnerability in their products?

2. BACKGROUND

2.1 Computer Ethics

What is "computer ethics", exactly? According to Professor Terrell Ward Bynum of Southern Connecticut State University, computer ethics is a part of practical philosophy that explores how technology professionals should decide how to behave in professional and social environments. Simply stated, computer ethics is the field of study which involves "systematizing, defending, and recommending concepts of right and wrong conduct[4]" in the field of computers and technology.

2.1.1 Norbert Wiener and the Beginning of Computer Ethics

The founding of the actual field of computer ethics actually occurred some time during World War II, in the early to mid-1940s. Norbert Wiener, a professor of mathematics and engineering at the Massachusetts Institute for Technology, is credited as being the founder of computer ethics even though the actual term "computer ethics" was only applied to the field decades later.

Wiener, along with colleagues from both the United States of America and Great Britain, helped "develop electronic computers and other new and powerful information technologies[6]," including an "anti-aircraft cannon capable of shooting down fast warplanes[7]." The anti-aircraft cannon used rudimentary computers to track and "perceive" an airplane, calculate where that airplane was heading, and then communicate this information to the part of the cannon responsible for aiming and firing the shells.

Quite advanced for its time, the challenge of this engineering collaboration led Wiener and his colleagues to create a new branch of science called "cybernetics[7]." Cybernetics, which deals with the science of information feedback systems, has only grown since Wiener and his colleagues started the field over sixty years ago. More important for this discussion, though, is the fact that the cybernetic study Wiener and his colleagues performed on their projects of the time led Wiener to write some "remarkably insightful ethical conclusions[7]" regarding computation in general.

With his mental faculties seemingly unclouded by wartime struggles, Wiener predicted that the world would undergo a sort of "second industrial revolution", something he called an "automatic age" with "enormous potential for good and for evil" that would bring with it myriad new ethical problems and opportunities[6]. Works later published by Wiener after World War II ended that explored his thoughts on the ethical implications of electronics and computers included *Cybernetics* (1948), *The Human Use of Human Beings* (1950), and his later book *God and Golem, Inc.* (1963). He explored ethical issues that continue to stay relevant today such as computers and security, computers and unemployment, responsibilities of computer professionals, computers for persons with disabilities, computers and religion, information networks and globalization, virtual communities, teleworking, merging of human bodies with machines, robot ethics, artificial intelligence[6].

Although Wiener was regarded as a kind of eccentric scientist whose views on the future of computers and their ethical implications were considered unrealistic and fantastic, his predictions finally proved reasonable to the general public approximately two decades later when computers actually started to make significant social and ethical impacts on the world. Wiener was truly a pioneer in the field of computer ethics.

2.1.2 The Three "Influences" of Computer Ethics

A professor in the Department of Mathematics and Computers at Georgia Southern University named Margaret Anne Pierce divided the ethical aspects of computer technology usage into three main driving forces:

1. The individual's personal code.
2. Any informal code of ethical conduct that exists in the work place.
3. Exposure to formal codes of ethics[5].

This is the model used by Pierce to illustrate how people make ethical decisions in both informal and formal settings:

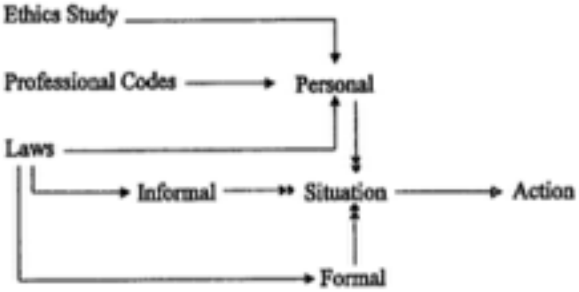

Figure 1: Pierce's model for personal ethics

In summary, ethics study and awareness of professional codes of ethics travel with the person in his or her memory. Both the ethical study, personal observations, and awareness/education of professional ethical codes influence the person's own code of ethics before he or she even arrives in a situation in which an ethical decision must be made. Additionally, a person has some level of understanding (anywhere between nonexistent and complete) regarding the legality of their choices in an ethical scenario they inhabit. Also, depending on whether the situation is informal or formal, the person engaged will determine whether or not the relevant laws should be respected and followed. After all of these factors are processed in a person's brain during a situation, a decision is made on how to behave. If the person has been educated with regards to all of the driving factors (ethics study, professional codes of conduct, and laws), then the person is indeed more likely to make an ethical decision even in situations where others might fail to make the right decision. Note, of course, that the *right* decision is relative. As professional settings and codes of conduct vary, the correctness of certain ethical decisions varies also.

Dissecting how a person makes ethical decisions into three major influences (personal code of ethics derived from observation and experience, the informal code of ethics in the workplace, and the formal code of computer ethics as outlined in company policies) will aid in the modeling and exploring of the ethical implications of the Internet of Things.

2.1.3 The Association for Computing Machinery Code of Ethics

The Association for Computing Machinery (ACM), a non-profit international learned society for computing founded in 1947 and with a current membership number of over one hundred thousand, is the largest scientific and educational computing society. With a strong understanding of enormous impact of computing in commerce, industry, government, medicine, education, entertainment, and society at large, the ACM created an official Code of Ethics that software engineers can commit to. The ACM's Code of

Ethics exists for the purpose of helping software engineers to “ensure, as much as possible, that their efforts will be used for good… and to make software engineering a beneficial and respected profession.” The Code contains eight Principles that apply to not only professional software engineers but also software educators, managers, supervisors, policy makers, and students:

1. Contribute to society and human well-being

   The first principle affirms an obligation to behave in a way that enriches society, protects fundamental human rights, and serves the well being of humanity and civilization. As software engineers deal with the development and maintenance of computational systems, an indispensible goal is to ensure that these systems minimize threats to health, safety, and privacy. Accordingly, software engineers should work to guarantee that their systems are not only safe, healthy, and private, but also are used to improve society overall.

2. Avoid harm to others

   In the context of computer ethics, “harm” may refer to any of these undesirable penalties: loss of property, loss of information, loss of privacy, property or personal or environmental damage. Thus, ethical software engineers do their best to prevent any of the previously stated undesirable penalties from happening to anyone as a result of the software engineer’s work or personal computation.

3. Be honest and trustworthy

   Honesty and trust go hand-in-hand and both qualities are inherent in clear and thorough communication. Ethical software engineers provide full disclosure when discussing important business matters, refrain from intentional coercion or manipulation, and will abstain from making purposefully deceptive and/or false statements regarding anything in the workplace.

4. Be fair and take action not to discriminate

   This principle dictates that ethical computer professionals refrain from discrimination on the basis of race, religion, sex, age, disability, or other such factors.

5. Honor property rights including copyrights and patent

   Usually, laws prohibit the violation of copyrights, patents, and terms of license agreements. However, in cases where software is not explicitly protected by such laws, software engineers should ensure to obtain proper authorization before distributing, duplicating, or using software with ambiguous or undefined usage terms.

6. Give proper credit for intellectual property

   Stealing work from others and claiming it as your own is unethical, even if such work is not explicitly protected by copyright, patent, or licensing agreements.

7. Respect the privacy of others

   Computer technology provides a platform in which privacy is threatened more than in any other communication platform. It is of utmost importance for computer professionals and software engineers to take all necessary precautions in securing user data from reaching the hands of unauthorized parties.

8. Honor confidentiality[7]

   When entering into a confidentiality agreement either explicitly or implicitly, one should honor their promise to withhold relevant information unless otherwise required by law or another principle of this Code of Ethics.

As outlined, computer ethics is a very relevant and important subject in the modern world. With this brief background on computer ethics, we are now ready to venture into the Internet of Things and its ethical implications.

2.2 The Internet of Things

2.2.1 Definition and Terminology

"The Internet of Things" (IoT) as a term or phrase was first coined by British technology pioneer Kevin Ashton in 1999, who is also responsible for cofounding the Auto-ID Center at the Massachusetts Institute of Technology (MIT), which "created a global standard for RFID and other sensors[8]." Ashton coined the term to "describe a system where the Internet is connected to the physical world via ubiquitous sensors[8]." Even today, the precise definition of what the "Internet of Things" exactly means continues to be debated. Conflicting sources from marketing material to academic journal articles provide sometimes-conflicting definitions.

For the purpose of this paper, the IoT refers to "the network of physical objects or 'things' embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices[9]."

2.2.2 Applications

The first application of the IoT concept was a Coca-Cola vending machine at Carnegie Mellon University connected to the Internet in 1982 that used its network connectivity to provide drink inventory and temperature data remotely[10]. Advances in Internet technology (specifically, IPv6's "huge increase in IP address space[10]") decades later allowed a far greater amount of "things" to be connected to the Internet. "Big Data", a "broad term for data sets so large or complex that traditional data processing applications are inadequate," is commonly discussed with the IoT because of the large amounts of data that IoT systems often produce, use, and manipulate. Applications of the IoT concept include:

1. Media

   Data mining, the process of extracting data from devices owned by an individual to better understand the individual and their relevant consumption habits, has enabled the media industries to tailor advertisements and articles specifically for individual recipients. With public consumption of IoT devices on the rise, the data-mining potential for the media has grown and will only continue to do so. Ultimately, the IoT extends media's opportunity to "measure, collect, and analyze an ever-increasing variety of behavioral statistics[11]."

2. Infrastructure management and environmental monitoring

   The IoT can provide valuable services to those responsible for managing urban and rural infrastructure such as bridges, roads, railway tracks, electricity lines and poles, telecommunications infrastructure, *and* those responsible for monitoring environmental variables such as air quality, water quality, earthquakes and other emergencies, soil, and even wildlife. Both of these applications utilize small, mobile, and Internet-connected (usually via cellular towers or satellite) devices that are often spread across large geographic areas. Large "fleets" of small, mobile devices can be used to gather data as well as control machinery remotely. This results in increased overall efficiency, reduced downtime, and reduced costs of operation.

3. Manufacturing

Manufacturing continues to benefit greatly from the IoT, with more and more specialized manufacturing processes being automated with the help of robots and computers. Networking machinery, sensors, and control systems together for industrial applications “enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks[12].” With the help of the IoT, manufacturing is not only becoming faster and more efficient, but also safer and *smarter*. Interconnecting the sheer amounts of sensors, robots, operator equipment, and service information systems produces an exponentially higher amount of data than was available to manufacturers before the IoT. Careful monitoring and analysis of manufacturing data is the foundation on which improvements to manufacturing processes are implemented.

4. Energy management

With the IoT, the era of people saying, “I accidentally left the oven on!” will be a distant memory. Marketers and engineers of the IoT aim to connect all energy-consuming devices to each other and to the Internet, allowing (once again) for each device to communicate and be controlled remotely. Sophisticated algorithms programmed by hard-working software engineers can utilize the “big data” generated from energy-consuming devices to intelligently model and predict usage patterns so that energy waste is reduced completely or almost completely. For example, the Nest™ thermostat (a “smart” thermostat already available to consumers) boasts that it “learns your schedule, programs itself and can be controlled from your phone. Teach it well and the Nest Thermostat can lower your heating and cooling bills up to 20%[13].” This type of waste-reduction can also be applied in industrial and corporate environments.

5. Medicine and healthcare

IoT devices can be used to monitor health locally or remotely via small, wearable devices that users can connect to different parts of their bodies. Smart watches already available on the market, for example, can already measure one’s heart rate, calories burned, steps taken, and altitude climbed. For people with serious medical conditions, more specialized devices are available on the market: blood sugar monitors, blood oxygen monitors, pacemakers, etc. Additionally, with the onset of nanotechnology (sensors and computers that are so small, microscopes are necessary to even observe them), virtually all data required by doctors to diagnose and prescribe treatments to patients will be available remotely. In the future, humans could even choose to purchase “augmentations” that would increase functionality of certain body parts or even extend longevity of those parts. The concept seems to verge into the realm of science fiction, but robotic prostheses are already becoming quite advanced with the help of the IoT.

6. Building and home automation

Imagine riding home from work in an autonomous, self-driving vehicle. Just after you’ve left the office, your smart home computer hub is already aware that you’re on your way home. Accordingly, it sets the thermostat to your desired temperature based on your previous habits as well as current climate. Just before you arrive home, the hub opens your garage door and turns on the garage light. Once you walk to your door to enter your home, your smart watch and smart door lock become aware of each other and, thus, your door unlocks. You walk inside and your lights are already on the way you like and the television program you want to watch is playing. Sounds like something from *The Jetsons*, but this reality is already readily available (even if not yet widely adopted). Aside from the aesthetic value, building and home automation also promises efficiency improvements.

7. Transportation

Transportation is one field that remains to benefit most from the IoT. Each transportation vehicle, be it a car, truck, bus, train, or even airplane, is, in itself, its own IoT network. Take a car, for example. A car is equipped with myriad devices that all contribute to the general functionality: audio equipment, an engine, batteries, electronics for controlling things such as windows and locks, data gathering sensors for diagnosing and repairing malfunctions, etc. The IoT aims to connect all of these devices so they may communicate with each other and with the Internet. Now that the car (individual vehicle) itself is an IoT network, with all of its devices communicating with each other, imagine a *fleet* of autonomous vehicles such as this working together as *its own* IoT network. The level of cooperation and communication provided by this new platform is astounding because of the new potentials for improvements to transportation in general, including: reductions or even absolute annihilation of slow traffic, improvements in safety (greater than 90% of traffic accidents occur due to human error, after all[14]), a significant increase of time regained by commuters (instead of driving, commuters can be productive, relax, etc.), a massive reduction in actual number of cars needed (most cars are parked for the majority of their lifetime; if cars could drive themselves, they could be working all the time for transportation), and a significant saving of energy as most autonomous cars will also be electric and charged via solar energy.

Applications of the IoT are seemingly endless. There are sure to be more applications unveiled as technology and research advances with time. Until then, this paper will focus on these applications in the analysis of the ethical implications of the IoT.

2.2.3 Three Main Vulnerabilities

A fair number of significant safety, security, and privacy problems exist in many IoT products. Generally speaking, there are three main goals that hackers strive to achieve with these IoT devices:

1. Capture, or take control of the device

2. Steal information

3. Disrupt service (Denial of Service [DoS])

The next section will explore these three vulnerabilities, the reasons for their existence, and the ethical solutions to the problems.

3. ETHICAL IMPLICATIONS OF THE INTERNET OF THINGS

3.1 Downfalls of Unethical Computing

The Association for Computing Machinery’s official Code of Ethics mandates that ethical computing professionals maintain safety, security, and privacy in their systems via the affirmations made in principles one, two, three, seven, and eight. The first principle is to “Contribute to society and human well-being” and the second is to “Avoid harm to others.” The third principle says to “Be honest and trustworthy” while seven says, “Respect the privacy of others.” Lastly, the eighth principle of the ACM’s official Code of Ethics reads, “Honor confidentiality.” All of these principles are necessary ethical foundations for the development of safe, secure products that respect the privacy of its users. However, these ethical decisions are often ignored, leading to the release of poor products into the technology marketplace.

A study conducted recently by HP Research reported that the “average Internet of Things gadget has an astounding 25 security flaws, and 70 percent have at least one such vulnerability[16].” Moreover, a set of attacks ran by a Columbia University study on both business and consumer IoT products (things like embedded systems for business and home entertainment systems, webcams, and Wi-Fi routers for consumers) discovered that only 2.46 percent of the business products—and an enormous 41.62 percent of the consumer products—were vulnerable to even amateur hackers[15]. “Even in those products that do have shields,” the study asserts, “the protections are often not enabled or are undermined by the use of default or weak passwords[15].”

Unfortunately, these problems often arise due to unethical decisions made by business leaders, engineers, developers, and computing professionals. Now, these problems, their root in poor professional ethics, and their ethical solutions will be outlined.

3.1.1 Haste, Laziness, and Ignorance

Due to the rapid nature of the growth of the IoT, many critics have claimed that developers are not dedicating an appropriate amount of their resources to the security and safety challenges in the IoT[15]. Consumer IoT product manufacturers are often too hasty to get their product(s) on the market, rushing their development process and leaving their products vulnerable. In addition to haste, some manufacturers also exhibit laziness as well as ignorance with regards to product safety and security. All three qualities are both unethical in business *and* contribute to poor-quality products that inhibit a company or business from achieving greater success.

The ethical solution to stopping products from being released too hastily (or lazily or with ignorance of security) involves educating business leaders, developers, and computing professionals about the importance of long-term investment in customer satisfaction. Products rushed to market may have the upper hand in the early days of a product category's lifespan, but, while many consumers may buy these rushed products, consumers will eventually come to lament the major flaws in said products. Products which were developed by lazy business leaders, engineers, and computer professionals are often sloppy, buggy, insecure, and unsatisfactory for customers. Products developed by computing teams lacking knowledge of security are bound to suffer from similar fates.

Consumers, with help of the media, learn about products they use and/or care about. In today's Age of Information, any manufacturer should absolutely not expect to have their mistakes and unethical decisions swept under the rug to pass by unnoticed.

Additionally, security is an important feature for many consumers. Releasing a hastily made, sloppy, and insecure product to the technology market will only have long-term negative consequences for the people and company who are responsible for it. Releasing poor products can tarnish brand name recognition, destroy the consumer trust relationship, and even put a company and its workers at risk of expensive litigation.

Meanwhile, companies who make *ethical* decisions (and practice patience and diligence in developing products that are secure and full of useful features) will ultimately come to dominate the market as technology media and consumers come to recognize the clear superiority of said products. Rushing products to market, being lazy in their development, or developing without security experts, are all clearly unethical *and* unsustainable business practices. The next section will specify the security measures an ethical business should take to ensure success.

3.2 Security Measures for Ethical IoT Product Development

To avoid releasing products that suffer from the three main vulnerabilities outlined in Section 2.2.3, here are some major security measures that an ethical business and computer professionals can utilize.

3.2.1 Firewalls

One of the easiest ways to stop hackers from achieving any of the three main goals (capture, steal, or disrupt) is to prevent them from communicating with the devices in the first place by implementing a firewall.

A firewall is basically a network security system (either hardware of software) that filters incoming and outgoing traffic according to customizable sets of rules. This rules-based network filtration system can prevent such things as unauthorized remote updates of embedded firmware and, on the other hand, allow authorized users administrator access via use of a "whitelist."

The resources required to run a firewall for an IoT product are minimal and can even be completely outsourced via a proxy server or a "bump in the wire" approach that simply adds a small, embedded computer in the IoT product's wire.

Firewalls are a decent start to securing IoT products but they are only appropriate for preventing capture and denial of service (DoS) attacks. To protect against data stealing and eavesdropping, other solutions must be implemented.

3.2.2 Encryption, passwords, and certificates

Without encryption, data is transmitted through networks in “clear text,” which means that anyone who manages to access the signal (either wireless or wired) will also be able to read the data without hesitation.

Additionally, even data that *is* encrypted may be at risk for eavesdropping if the passwords used to encrypt the data are weak. Many devices (such as Wi-Fi routers and access points) use appropriate encryption algorithms (like AES-256) for data transmission but fail to require the usage of strong administration passwords. In such cases, all a hacker needs to do to obtain access to the content of data being transmitted is type in a default password.

Since Edward Snowden started leaking classified government and National Security Agency (NSA) documents that revealed their widespread violation of Americans’ 4th Amendment right to privacy, the public’s demand for privacy has skyrocketed. According to a survey conducted by the Pew Research Center, “80% of adults ‘agree’ or ‘strongly agree’ that Americans should be concerned about the government’s monitoring of phone calls and internet communications. Just 18% ‘disagree’ or ‘strongly disagree’ with that notion[17].”

For people who are deeply concerned with privacy in technology and the Internet, simply implementing data encryption in their products is not enough to satisfy. Although many people trust (or would like to trust) companies to make ethical decisions with regards to privacy, the public cannot verify that a product or service protects their privacy unless the privacy measures taken in said product is *open to peer-review*. The best practices for data encryption, after all, are *open-source*, meaning that the source code is freely available to view and use. Without that openness, people must trust a company to protect their privacy, and, as Snowden’s leaked documents continue to illustrate, trust is not good enough.

Lastly, certificate-based authentication provides yet another means of protecting user data from being leaked to unauthorized parties. Without venturing too deeply into the technicalities of this security measure, certificate-based authentication systems essentially obtain a user’s password, hashes it with an encryption algorithm, then uses the hash plus other client-specific data to create a unique certificate that is then sent to a server for verification. If the server recognizes the certificate it receives, the client’s identity is authenticated and communication between the two can continue.

Ethical business decisions with regards to privacy in IoT products mandate that strong, open-source encryption and/or certificate-based authentication standards are implemented, strong passwords are *required*, and firewalls are provided as a default option.

3.2.3 Emerging standards for IoT security

There are a number of standards for IoT security emerging from various committees and consortiums. Two groups, The Industrial Internet Consortium and The Open Interconnect Consortium, exist primarily to ensure that the “non-consumer IoT[16]” technologies used by different companies can communicate with each other. Members of both consortiums are working on security features that will be built into their reference architectures and technologies and thoroughly documented in the process[16].

A number of Institute of Electrical and Electronics Engineers (IEEE) standards also exist for certain elements of security:

- IEEE P1363, a standard for public-key cryptography.
- IEEE P1619, a standard for encrypting data on storage devices like hard drives.
- IEEE P2600, a standard for securing office devices like printers and copiers.
- IEEE 802.1AE and IEEE 802.1X, standards for “media access control security[16].”

One of the world’s most widely adopted family of technology security standards is The International Standards Organization’s (ISO) ISO 27000. A team working for ISO called the Special Working Group on the Internet of Things plans to help “guide their [IoT products] evolution to better account for security[16].”

More standards for security exist and are easily accessible with Internet searches. Complying with standards is the best means for ensuring secure products.

4 CONCLUSION

The concept of the Internet of Things has introduced a great deal of new functionality as well as improved efficiency in already-existing systems. From automation to big data, the IoT has cemented a prominent place in technology innovation for at least the foreseeable future. However, it is often too easy for companies and computing professionals to make unethical decisions when developing and selling IoT products. These unethical decisions lead to poor security, safety, and privacy in IoT products. All IoT product manufacturers should instead take great care in making the right decisions during product development. To ensure safety, security, and privacy, computing professionals should review the Association for Computing Machinery’s official Code of Ethics, educate themselves on the robust standards available for implementation from the IEEE, and dedicate appropriate resources to ensuring ethical product releases.

REFERENCES

[1] Bynum, Terrell Ward. 2008, Aug. A Very Short History of Computer Ethics. Southern Connecticut State University. New Haven, CT. [Online]. Available: http://web.archive.org/web/20080418122849/http://www.southernct.edu/organizations/rccs/resources/research/introduction/bynum_shrt_hist.html

[2] Covington, M.J.; Carskadden, R., "Threat implications of the Internet of Things," *Cyber Conflict (CyCon), 2013 5th International Conference on*, vol., no., pp.1,12, 4-7 June 2013. http://0-ieeexplore.ieee.org.torofind.csudh.edu/stamp/stamp.jsp?tp=&arnumber=6568380&isnumber=6568361

[3] Crump, Catherine; Harwood, Matthew. The Net Closes Around Us. March 2014. [Online]. Available: http://www.tomdispatch.com/post/175822/tomgram%3A_crump_and_harwood%2C_the_net_closes_around_us/

[4] Fieser, James. Ethics. Internet Encyclopedia of Philsophy. University of Tennessee at Martin. Martin, TN. [Online]. Available: http://www.iep.utm.edu/ethics/

[5] Pierce, Margaret Anne; Henry, John W. (April 1996). Computer ethics: The role of personal, informal, and formal codes. *Journal of business ethics* **15** (4): 425–437. [Online]. Available: http://www.springerlink.com/content/m3201253822641r0/

[6] Bynum, Terrell Ward. Computer and Information Ethics. *The Stanford Encyclopedia of Philosophy* (Winter 2014 Edition), Edward N. Zalta (ed.). [Online]. Available: http://plato.stanford.edu/archives/win2014/entries/ethics-computer/

[7] Agarwal, S.; Garcia, M., "What to Teach About Computer Ethics," *Information Technology Based Higher Education and Training, 2006. ITHET '06. 7th International Conference on*, vol., no., pp.86,93, 10-13 July 2006. [Online]. Available: http://0-ieeexplore.ieee.org.torofind.csudh.edu/stamp/stamp.jsp?tp=&arnumber=4141612&isnumber=4084515

[8] McHugh, Josh. Attention, Shoppers: You Can Now Speed Straight Through Checkout Lines! *WIRED Magazine*. July 2004. [Online]. Available: http://www.wired.com/wired/archive/12.07/shoppers.html

[9] “Internet of Things”. Wikipedia. June 2015. [Online]. Available: https://en.wikipedia.org/wiki/Internet_of_Things

[10] Frank Palermo. Internet of Things Done Wrong Stifles Innovation. InformationWeek. 7 July 2014. [Online]. Available: http://www.informationweek.com/strategic-cio/executive-insights-and-innovation/internet-of-things-done-wrong-stifles-innovation/a/d-id/1279157

[11] Moss, Jamie. The internet of things: unlocking the marketing potential. The Guardian. June 2014. [Online]. Available: http://www.theguardian.com/media-network/media-network-blog/2014/jun/20/internet-things-marketing-potential-data

[12] Ersue, M; Romascanu, D; Schoenwaelder, J; Sehgal, A (4 July 2014). "Management of Networks with Constrained Devices: Use Cases". IETF Internet Draft.

[13] Marketing material. Life with Nest Thermostat. 2015. [Online]. Available: https://nest.com/thermostat/life-with-nest-thermostat/

[14] Smith, Bryant Walker. Human Error As A Cause Of Vehicle Crashes. The Center for Internet and Society. Stanford Law School. December 2013. [Online]. Available: http://cyberlaw.stanford.edu/blog/2013/12/human-error-cause-vehicle-crashes

[15] Clearfield, Chris. Why The FTC Can't Regulate The Internet Of Things. Forbes. September 2013. [Online]. Available: http://www.forbes.com/sites/chrisclearfield/2013/09/18/why-the-ftc-cant-regulate-the-internet-of-things/

[16] Grau, A. Can you trust your fridge? Spectrum, IEEE, vol.52, no.3, pp.50,56, March 2015. [Online]. Available: http://0-ieeexplore.ieee.org.torofind.csudh.edu/stamp/stamp.jsp?tp=&arnumber=7049440&isnumber=7048071

[17] Madden, Mary. Public Perceptions of Privacy and Security in the Post-Snowden Era. Pew Research Center: Internet, Science, & Tech. November 2014. [Online]. Available: http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/