What Role Should Government Regulation Play in Regulating IoT?

Regis University

Billy Hansen

Regulating the Internet of Things

Introduction

Older relatives often reminisce about what life was like before the Internet or smart phones. It's likely that millennials will someday tell their children about life before the Internet of Things (IoT). There's no universal definition of IoT, but the most basic description is a smart environment, where instantaneous connectivity expands beyond smart phones and laptops to everyday objects like clothing, home appliances, cars, and exercise equipment, to name a few. IoT will include autonomous decision making, guided by big data insights and machine learning (Helen et al. 2013).

Predictions show that the IoT will become a multi-trillion dollar market (Habibi, J., Midi, D., Mudgerikar, A., & Bertino, E. (2017). If created and used successfully, the IoT could guide a user toward a happier, more fulfilled life (Helen et al. 2013). It could provide real time medical diagnoses, help avoid risks and threats, and offer vast new options for entertainment (Helen et al. 2013). It's also widely speculated that applications beyond our current understanding will emerge (Peppet, 2014). Therefore, there are powerful incentives to build such an environment.

However, the IoT comes with significant risks to privacy and security. Hacking and cyber-attacks have already become commonplace, and as IoT develops and expands, many speculate that it will become increasingly vulnerable to such attacks, and that the attacks will be more consequential (Helen et al. 2013). Another concern is the ethical implications that will accompany such technological advancements. Bailey (2016) argues that when a user purchases an IoT device, he or she is sacrificing some of his or her privacy. When data is constantly being shared across multiple devices (i.e. phone, computer, roads, cars, exercise equipment, medical monitoring devices, shoes, etc…), and across platforms and within different companies and

organizations, how would it be possible for users to offer consent for all data being recorded about their behavior (Popescul & Georgescu, 2013)? Will privacy cease to exist?

Even though the potential risks of privacy infringement and faulty security are significant, there doesn't appear to be a likely way to slow or halt the creation of a fully connected IoT environment. Instead, there is strong motivation to keep improving our technology, often fueled by the money to be made by breaking new ground in the IoT domain (Bo & Yulong, 2017). Therefore, debating whether we should create an IoT environment becomes a moot point, and instead research needs to stress building the system in an ethical and efficient way. To do so, the IoT environment must, among other things, protect itself from hacking, and be regulated so as to meet ethical and practical standards – standards that have yet to be created or agreed upon universally.

Purpose

It is necessary to begin development of the IoT environment with principled standards in order to see ethical results that foster a healthy and thriving IoT environment. The purpose of my study is to explore what role government should play in regulating the IoT environment. I'll compare and contrast differing suggested methods drawn from previous research on the topic. I'll also show that the most convincing research from sources like Peppet (2014), and Valacich and Schneider (2010) suggests the following: The purpose of government regulation should be to meet ethical standards regarding privacy, non-discrimination, and freedom of speech and expression – standards that will become increasingly difficult to achieve in a fully connected IoT environment. Governments must also be careful not to stifle the growth of the IoT through overregulation (Helen et al. 2013).

Significance

How much control of the IoT environment should the government have? Some argue that government intervention is necessary in order to achieve an open, collaborative creation between developers of IoT products and services (Poudel, 2016). Others argue that without breaking up the siloed creation of IoT products and services within individual companies, the IoT is far less likely to be successful because the products won't cohere to a secure and fair system of development (Poudel, 2016). Helbing and Pournaras (2015) offer a counter-argument to this premise: that if an unethical, opportunistic, or corrupt government controls this powerful data, a totalitarian regime could result, and that the system could be most successfully regulated with ethical guidelines contained in the code that the IoT is built with (Peppet, 2014).

Fostering an IoT environment that contributes to thriving, free societies requires that ethical standards be set and met. IoT will force us to clarify our ethical priorities, and it is urgent that we do so. If the ethical guidelines in the IoT environment lag too far behind rapid improvements in technology, IoT will likely not be as beneficial as it could be. This study is an attempt to explore various methods of how government can help guide the IoT toward a positive end. Gaps in prior research will be identified as a means of encouraging future research on the topic.

Literature Review

According to Zaslavsky and Perera and Ceorgakopoulos (2012), The Internet of Things is predicted to add approximately $300 billion annual value to the US health care system; approximately "$600 billion annual consumer surplus" as a result of sharing personal location data globally; approximately "60% increase in a retailers' operating margin"; and a demand for 1.5 million additional data-proficient employees (p.4). A consumer surplus of $600 billion means

that consumers would be willing to pay $600 billion more than they are actually paying for IoT products, which would make the demand to offer the technology extremely high. The companies that are proactive and willing to adapt to an IoT environment will be at a great advantage (Bo et al, 2017). This profit motive makes the concept of voluntarily stopping the creation of an IoT environment virtually impossible. Therefore, all possible effort and energy in regulation should be spent attempting to steer the IoT environment in the best available direction. Before comparing potential government regulation methods for the IoT environment, it is important to discuss what the government should be aiming to accomplish. And it should be noted that with the rapid growth of the IoT environment, there is significant urgency to grow and modify laws and regulations related to IoT (Poudel, 2016).

An area of concern amongst IoT researchers is the security of such a connected environment (Habibi et al. 2017). We are already noticing the vulnerability of our connected world as cyber-attacks become commonplace. Some examples of recent cyber infiltration include the seizing of hospital networks and demanding cryptocurrency as ransom, blackmail through email and personal information infiltration, and, perhaps most notably, the Russian hacking of the 2016 US general election. Habibi et al. (2017) describe how the power of cyber-attacks and thievery is expanding rapidly. Malicious botnet software designed to infiltrate networks and hardware devices in order to cause harm and steal valuable information is becoming increasingly difficult to combat. Habibi et al. (2017) claim that botnets using many comprised machines have massive amounts of bandwidth and computing capability enabling them to auto-scan networks for weak passwords to crack.

As Zasalavsky et al. (2012) pointed out, because of the potential value of the IoT there will likely be great incentive to use malicious software to infiltrate and steal information.

Currently, hacking is a low risk high reward activity, because it's so difficult to identify hackers (Zasalavsky et al., 2012). Key objectives of government should be protecting the IoT environment from attacks, and identifying gaps in IoT security (Mineraud et al., 2016).

There are many ethical concerns in anticipation of the IoT environment, and some researchers argue that a successful IoT will hinge on meeting ethical standards so consumers can trust and support such a connected world (Helen et al., 2013). Therefore, governments should also be concerned with fostering an ethical environment. A definition of what this ethical standard should be is shown below. Helen et al. (2013) discusses how our intuitions about human rights to privacy will likely be altered as IoT emerges. If the IoT environment develops as it is expected to, private lives might cease to exist. Sensor data in smart phones and other IoT can already infer much about the user (Poudel, 2016). IoT data will likely be able to predict a user's driving habits, mood, stress levels, personality traits, gender, marital status, risk for various diseases, smoking habits, and exercise habits (Poudel, 2016). There's also great risk that hacked IoT devices could give outside access into a user's personal space at home (Poudel, 2016).

The IoT could lead to discrimination in ways we haven't yet contemplated. A relevant example was given by Bersin et al. (2017), who explained how modern world class athletes quantify a number of variables like sleep, caloric intake, weight lifted, miles traveled, and water consumed. They use this data to optimize their performances. Bersin et al. (2017) argue that in an IoT environment this type of optimization will become commonplace for what they call "corporate athletes" (p. 60). "Corporate athletes" are those who optimize their work and personal life through analytics (Bersin et al. p. 60). While these data driven optimization practices will help people organize and improve their lives, the benefits might come with a cost. There will also be incentives for employers to quantify their employees, as evaluating employees based on

efficiency will empower companies to make more data-driven decisions about them (Bersin et al. 2017). But this data collection will require extensive surveillance of employee behavior, and will likely lead to resistance from employees who don't want their every move known (Bersin et al. 2017). This practice is referred to as "talent analytics", which could be helpful for employers to optimize their workforce, but could inadvertently lead to automated systems using variables like race, gender and age to choose preferable employees, which is explicit discrimination (Peppet, 2014, p. 118).

Another example of ethical concerns as IoT develops is how it will affect healthcare and medical treatment (Mittelstadt, 2017). The potential benefits are extraordinary, as patients with conditions that have previously forced them to spend extensive time at the hospital will instead be able to live more normal lives at home while being monitored by IoT health related applications (Mittelstadt, 2017). The devices can also encourage healthy habits, detect disease and even recommend checkups and preemptive measures when disease is anticipated (Mittelstadt, 2017). However, with all of this available data about individuals' health, will that data also be used by employers and life insurance companies (Mittelstadt, 2017)? If an automated system estimates that an individual has a significant chance of dying by age 50, that person would have a difficult time finding affordable life insurance, and if potential employers have this information an applicant may have an unfair disadvantage finding a job. Also, Mittelstadt (2017) worries that this type of remote treatment might not offer patients the emotional and human support that our current doctors and nurses provide, leaving patients isolated and at greater risk of depression.

User consent and awareness is another pressing issue in an IoT environment. Popescul and Georgescu (2013) argue that the IoT system will be so complex, and data will be shared across

so many devices, that user consent will be nearly impossible to establish. There will be great discrepancy over who owns the data, and because public awareness and consent will be so difficult to verify and enforce, many ethical breaches may go undetected (Popescul & Georgescu, 2013). Peppet, (2014) posed the following difficult question: "How should the law treat—and how much should policy depend upon—consumer consent in a context in which true informed choice may be impossible?" (p. 85).

Government regulation should attempt to combat these potential ethical and security concerns without stifling the growth of IoT. Before comparing potential strategies for how this could be accomplished, it is also important to discuss the most pressing goals that have been identified in previous research. Peppet, (2014) lists what he believes are the "Four Problems" with the development of IoT: "Discrimination", "Privacy", "Security" and "Consent" (p. 86). And, according to authors Valacich and Schneider (2010), an ethical behavior in the space of IoT requires that we "enforce the property rights on information; ensure the access to information; ensure the integrity of the information; enforce the right to private life (p. 484)."

These standards simply and concisely state what the objectives should be in regulating the IoT environment. When comparing government regulation methods, these will be the objectives we consider. How should a government approach regulation so IoT can grow to its potential without allowing it to abandon these acute ethical concerns?

If the IoT environment is going to grow and reach the anticipated value, then the "things" (connected devices) in the IoT environment must be able to "interoperate" with each other (Poudel, 2016). IoT won't reach its full value, or be sufficiently resistant to security breaches, if "things" from different companies don't connect and share data automatically (Poudel, 2016). Because of this, Poudel, argues that IoT won't reach its potential unless a "global standardized

platform" is created (p. 1009). If the global standardized platform creation is left to the free market, which seems not only inevitable, but preferable, so that competition can spark innovation and growth, then there are three prevailing options for how this market will come about (Poudel, 2016). While the free market will drive IoT growth, it is important to consider how free market development might take place when deciding how to guide the IoT with government regulation. The first requirement would be a system in which leading firms choose incompatibility between networks and devices, which would lead to a race to become the dominant platform (Poudel, 2016). The second requirement would be firms agreeing on common standards, with debate about what the standards should be depending on what would benefit each firm. The third requirement would be that the dominant firm creating the platform should try to exclude other firms from that platform, while smaller firms try to make their systems compatible to the dominant firm's (Poudel, 2016).

To what degree should governments attempt to control the development of the IoT? Three different methods will be compared – very little or no regulation, firm regulation, and moderate regulation, or what Helen et al. (2013) calls "soft law".

It is important that governments give the IoT space to grow (Helen et al. 2013). If governments attempt too much regulation, then the market for IoT will simply grow elsewhere, leaving the countries with overly cautious governments at an economic disadvantage (Helen et al. 2013). Stifled growth is the primary argument for why regulating IoT would be unwise (Helen et al. 2013). Another argument for little or no regulation is the idea that the IoT would be better suited to regulate itself for ethical and security problems. Habibi et al. (2017) suggest that the best way to address security breaches is a safeguard built into the system. As stated above, the complexity of IoT might leave many security breaches and ethical breaches undetected,

which of course wouldn't be addressable by a government (Habibi et al. 2017). Habibi et al. (2017) propose a defense mechanism called Heimdall that attempts to safeguard against malicious software by using what Habibi et al. (2017) call "whitelisting". Whitelisting is a system that compiles lists of all the various "things" that a device can reach. It uses statistical data to monitor the incoming and outgoing functions of the device and regulates for normality (p. 3). The multilayered incoming and outgoing defense can stop infiltration from occurring even if malware is able to penetrate one layer of defense (Habibi et al. 2017). Habibi et al. (2017) then evaluate their proposal and argue that it should be the basis of what we create to protect IoT. It is important to point out that little or no regulation is the system we currently have in most countries, so if nothing is done, this is the approach that will play out (Helen et al. 2013).

The disadvantages for little or no regulation are simply that an unfettered IoT environment might end up as vastly unethical (Helen et al. 2013). The free market would yield winners and losers leading to greater levels of income inequality, discrimination, and a lack of privacy (Helen et al. 2013). Without government regulation on privacy standards, there might not be such a thing as privacy remaining (Helen et al. 2013). There is also great concern that an uninhibited IoT network might take the form described as the first option above, where firms are not willing to collaborate and build a platform that yields automatic connectivity (Poudel, 2016). If this concern turns out to be valid, then government guidance towards platform regulations might be the only way IoT reaches its full potential and growth (Poudel, 2016). For these reasons, many researchers believe strict government intervention is the only feasible way forward (Helen et al. 2013).

Most researchers agree that a balance must be struck between self-regulation and periodic government intervention (Helen et al. 2013). There's a consensus that human establishments

won't have the bandwidth or speed to catch all security breaches or ethical breaches (Habibi et al. 2017). The appropriate middle ground might be for a government to require adequate code in the IoT framework to catch discrimination, privacy breaches, and areas of risk for security breaches (Helen et al. 2013).

It is also dangerous to think that a "good" government should have control and access to all data in the IoT (Helbing & Pournaras, 2015). Helbing and Pouraras discuss how totalitarian governments or authoritarians will likely use this data insight to further cement their power, and, in many cases, further oppress their people. They also discuss how even governments with benign or good intentions could still contribute to an unethical system. It gives an example of how citizens could be ranked based on their internet activity, and how China has already implemented this type of evaluation system (Helbing and Pouraras, 201). This problem isn't unique to government data control, as Helbing and Pouraras (2015) discuss in the following quote:

Many policymakers believe that personal data may be used to 'nudge' people to make healthier and environmentally friendly decisions. Yet the same technology may also promote nationalism, fuel hate against minorities or skew election outcomes if ethical scrutiny, transparency and democratic control are lacking — as they are in most private companies and institutions that use 'big data'. The combination of nudging with big data about everyone's behavior, feelings and interests ('big nudging', if you will) could eventually create close to totalitarian power. (Helbing and Pournaras, 2015, p. 1).

This indicates that checks and balances should be in place. For IoT to reach its potential, governments should try to foster an open and collaborative creation of IoT (Poudel, 2016). Helen et al. (2013) suggest the "soft law" approach (p. 99), wherein governments use "measures other than changes to laws and regulations to stimulate development and mitigate problems in some areas and observing other areas, possibly leading to later action (p. 99)."

Another option for government regulation (Kennedy, 2016) actually turns the dynamic on its head. Instead of using government to monitor the IoT, Kennedy, (2016) suggests the possibility of using IoT technology and artificial intelligence (AI) as the government itself to regulate and mandate society. Governments have already started incorporating AI as a strategy in their own government practices. AI (in its current form) isn't influenced by emotions that typically contribute to human stupidity in governance (greed, jealousy, lust, illness etc..) (Kennedy, 2016). AI is already superhuman in computation, data storage, and speed of information processing (Kennedy, 2016). It is easy to see why it might be enticing to create a "smart government."

Kennedy, (2016) decides that while there are many foreseen advantages of a potential "smart government," it would likely come with shortcomings as well. The primary shortcoming is expected to be a lack of flexibility. The AI system would stick to the code 100% of the time, and it would be unable to use common sense while enforcing rule of law unless common sense is coded into the system (Kennedy, 2016). A helpful hypothetical example of this lack of common sense was given by Bostrom, (2016), when he described a situation when a super artificial intelligent machine was commanded to stop all spam emails. Without common sense being coded into the machine, it might decide to eliminate the source of all spam emails, which are the human beings that create them.

Conclusion

If history is any indication, many of the coming innovations in IoT and AI technology are unpredictable (Magruk, 2016). In fact, Magruk, (2016) argues that the new innovations will be changes no one is currently thinking about, and uses examples like the internet and the IPhone as examples of improvements that very few had anticipated.

So what strategy should governments apply to regulating IoT? While the "smart government" method seems intriguing because of its superhuman bandwidth, computing ability, and speed, it still requires IoT and AI technology to improve considerably before the idea becomes possible (Kennedy, 2016). Therefore, we will still need human guidance for IoT to develop in the interim. Because of the uncertainty that Magruk, (2016) describes, the government strategy that should be implemented is what Helen et al., (2013) describes as "soft law" or "quasi-law" over the IoT. This flexible governance should aim to give IoT room to grow to its full potential, while staying prepared to enforce course corrections when ethical breaches, security vulnerabilities, or platform disputes arise (Helen et al. 2013). The research indicates that governments won't be able to effectively catch ethical or security breaches, and it would be better served monitoring the code that can detect them from within the IoT environment (Habibi et al. 2017).

Much of the focus in future research should be focused on platform creation in IoT (Mineraud et al. 2016). Mineraud et al. (2016) stresses that a successful IoT environment would be built on a platform ensuring user privacy and security, with enough flexibility so that it can change and adapt. This flexibility is crucial if responsible governments are to be able to intervene when necessary (Helen et al. 2013). Mineraud et al. (2016) argue that the most crucial gap in IoT platform development is how it will allow for data reusability, and how data that is being reused

can still ensure data privacy. After reviewing the prominent platforms that are currently in development, Mineraud et al (2016) identifies “EveryWare” as the leader in terms of ensuring adequate flexibility, privacy, and security (p. 8). While researchers have differing ideas on how IoT should develop, there is a consensus around the fact that more thought, effort and research need to be done, in order to build a truly successful IoT environment.

References

Bailey, M. W. (2016). Seduction by technology: why consumers opt out of privacy by buying into the internet of things. *Texas Law Review*, *94*(5), 1023-1054. Retrieved from Bailey, M. W. (2016). Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things. Texas Law Review, 94(5), 1023-1054.

Bersin, J., Mariani, J., Monahan, K., & Winn, B. (2017). Will employees be the next cloud connected "thing" in the new era of IoT?. *People & Strategy*, *40*(3), 60-64 Retrieved from http://web.b.ebscohost.com.dml.regis.edu/ehost/detail/detail?vid=4&sid=4df9569c-c243-4b2e893d2ddb0facbb0e%40sessionmgr104&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=123988601&db=bth

Bo, L., & Yulong, L. (2017). Internet of things drives supply chain innovation: a research framework. *International Journal Of Organizational Innovation, 9*(3), 71-92. Retrieved from http://web.b.ebscohost.com.dml.regis.edu/ehost/pdfviewer/pdfviewer?vid=2&sid=a5fcada3-4a60-4acd-a502-352a244fcf79%40sessionmgr104

Bostrom, N. (2016*). Superintelligence: paths, dangers, strategies*. New York: Oxford University Press.

Habibi, J., Midi, D., Mudgerikar, A., & Bertino, E. (2017). Heimdall: Mitigating the internet of insecure things. *IEEE,* PP (99), 1 – 11 Retrieved from https://www.researchgate.net/publication/317032003_Heimdall_Mitigating_the_Internet_of_Insecure_Things

Helbing, D., & Pournaras, E. (2015). Society: Build digital democracy. *Nature, 527*(7576), 33-

34. doi:10.1038/527033a

Helen, S., & Cave, J. & Robinson, N. & Horvath, V. & Hackett, P. & Gunashekar, S. & Maarten, B. & Forge, S. & Graux, H. (2013). Europe's policy options for a dynamic and trustworthy development of the internet of things. *Rand, xv-152*. Retrieved from https://www.rand.org/pubs/research_reports/RR356.readonline.html

Kennedy, R. (2016). E-regulation and the rule of law: Smart government, institutional information infrastructures, and fundamental values. *Information Polity: The International Journal Of Government & Democracy In The Information Age*, *21*(1), 77-98. doi:10.3233/IP-150368

Magruk, A. (2016). Uncertainty in the sphere of the industry 4.0 - Potential areas to research. *Business, Management & Education / Verslas, Vadyba Ir Studijos*, *14*(2), 275-291. doi:10.3846/bme.2016.332

Mineraud, J., Mazhelis, O., Su, X. & Tarkoma, S. (2016). A gap analysis of internet-of-things platform. *Computer Communications*, *89*, 5 – 16. Retrieved from https://doi.org/10.1016/j.comcom.2016.03.015

Mittelstadt, Brent. (2017). Ethics of health-related internet of things: a narrative review. *Ethics and Information Technology*. Retrieved from https://link.springer.com/article/10.1007/s10676-017-9426-4

Peppet, S. R. (2014). Regulating the internet of things: first steps toward managing discrimination, privacy, security, and consent. *Texas Law Review*, *93*(1), 85-178. Retrieved from http://web.b.ebscohost.com.dml.regis.edu/ehost/pdfviewer/pdfviewer?vid=5&sid=a5fcada3-4a60-4acd-a502-352a244fcf79%40sessionmgr104

Popescul, D. & Georgescu, M. (2013). Internet of things – some ethical issues. *The USV Annals of Economics and Public Administration, 2(18),* 208-214. Retrieved from http://seap.usv.ro/annals/ojs/index.php/annals/article/viewFile/628/599

Poudel, S. (2016). Internet of things: underlying technologies, interoperability, and threats to privacy and security. *Berkeley Technology Law Journal, 31*997-1021. doi:10.15779/Z38PK26

Valacich, J., Schneider, C., (2010), Information Systems Today. Managing in the Digital World, *Ediţia* a 4-a, Editura Pearson, Boston

Zaslavsky, A., Perera, C., Georgakopoulos, D. (2012). Sensing as a service and big data. *Proceedings of the International Conference on Advances in Cloud Computing (ACC). India*. Retrieved from https://arxiv.org/abs/1301.0159