A Framework for Emotion and Trust Between Humans and the Internet of Things

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Bryan Rombach
Spring, 2020

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____ Date _____
Bryan Rombach

Approved _____ Date _____
Bryn Seabrook, Department of Engineering and Society

The Internet of Things is Growing

As technology progresses, devices will increasingly be woven into our daily lives. The interconnection of small computers embedded in everyday objects, known as the Internet of Things, has been growing for more than a decade (Stevenson & Lindberg, 2011). That growth is expected to increase exponentially in the next decade; by 2035 more than a trillion devices are predicted to be connected. Known as the Internet of a Trillion Things, this will have an average of more than 100 devices per person on earth (Perry, 2019).

These technologies should improve our day-to-day life by introducing efficiencies, informing decisions, and enhancing communications, but they also stand the risk of instigating a deep-seated negative human emotion: distrust (Ahmed, Ab Hamid, Gani, Khan, & Khan, 2019). If trust in the Internet of Things is lost, the technology will be rejected in a way which is difficult to recover from, stifling technological progress and the improvements it brings.

This paper uses Actor-Network theory and technological momentum analysis to investigate the consequences of deep integration between the internet, physical devices, and our society. Government, private businesses, and consumers must work together to reach this integration in a way which brings improvements to all.

Analyzing Past Failure

How can Internet of Things devices be designed, integrated, and managed in a way that inspires trust in users? This paper develops a framework which serves to guide companies to success and proposes a complementary set of regulatory restrictions which will protect consumers from abuses by technology firms. Previous works have analyzed the issue of trust, but

have primarily focused on how a person can determine whether or not to trust a device rather than how companies can design and sell trustworthy devices (Fritsch et al., 2012; Xia et al., 2019). Examining a historical example of a pair of similar technologies in which one failed and one succeeded with the general population, implementation differences are examined to find issues where human trust may have played a role. A wicked problem framing drives the composition of evidence and the understanding of why this is such a difficult problem.

Technology as a Part of Life

The generation entering adulthood now has had computer technology present for a large portion of their lives, but grew up alongside it rather than *with* it. The portable personal computers which would lead to smartphones were in their infancy twenty years ago, same as those adults. Today, toddlers are getting some of their first education from iPads and adults working in nearly every sector of the economy rely on mobile technology. In the home, a thermostat can run autonomously, a doorbell camera can be viewed from a smartphone anywhere in the world, and a voice command can turn lights on in any hue—facts unimaginable a decade ago. Yet, the future is much more immersive than that. As compact, energy efficient, wireless devices mature, they will be integrated ubiquitously into daily lives. Almost any item that a person interacts with stands the chances of becoming connected, from a coffee mug to a car tire, and this fact has widespread implications for personal privacy and mental well-being.

The technology used in our daily lives is transforming from a simple tool for accomplishing work to something much more profound which is intrinsically connected to our emotional state. In 2011, surveyed users spent an average of 46 minutes a day using their mobile

devices. By 2015, that number had risen to 2 hours and 54 minutes ("Growth of Time Spent on Mobile Devices," 2015). Walking around on any given day, it is easy to see the enormous number of users interacting with their smartphones. More difficult to see is the growing number of interactions which people have with Internet of Things devices. These interactions may be passive, such as one's thermostat detecting their departure and adjusting the temperature to save energy, or active interactions, such as asking a smart home speaker what the weather will be like before picking an outfit for the day. Whereas a phone is often central to a given moment, the Internet of Things lies in the periphery and can affect a person in subtle but impactful ways (Montag & Diefenbach, 2018).

Today, the Internet of Things remains slightly out of reach, and perhaps under-useful, for the average consumer. Prices will continue to drop, technology will continue to improve, and the smart home will become just as common as the smartphone. As the Internet of Things grows in the home and overflows into our cities and workplaces, its presence will eventually affect every person who lives in a modernized society (Gudur, Blackler, Popovic, & Mahar, 2013). Any device which is useful to us today stands the chance of becoming internet-connected, and many new use cases will arise which we would never consider today (Ashford, 2014). Behind this wave of growth will be startups, new companies filling the spaces, but also the technology companies we know today: Apple, Google, Amazon, Facebook. Backing the hardware will be more big players: the telecommunications companies. Internet Service Providers such as Charter, Cox, and Comcast and cellular providers such as AT&T, Verizon, and Sprint. Finally, linked to both the consumers and the large companies will be the governments which will inevitably need

to step in to regulate certain aspects of IoT devices and perhaps entire segments of the business such as smart cities (Lo & Campos, 2018).

Actor Network Theory and Technological Momentum

Society has never been so closely connected to technology as it has today, and the Internet of Things will only continue to deepen that connection. STS theory is well suited to examine this partnership, as it has for decades since its inception. In this paper, Actor-Network theory and the theory of technological momentum are used. Some scholars argue that Actor-Network theory does not account for pre-existing structures, instead assuming that everything is actively emerging from relationships (Whittle & Spicer, 2008), but the addition of technological momentum analysis will be used to make up for these shortcomings. Additionally, to deal with the lack of determinism in Actor-Network theory, I will be tightly scoping the components of the network to deal specifically with the user-device interaction in a home setting—the area which requires among the highest trust (Coughlan et al., 2012). This narrow scope will allow me to manage the number of connections and pull out meaningful conclusions. I will be using technological momentum to investigate the overarching societal players; big companies, government, and long lasting physical hardware are slow moving entities which are resistant to change but can absorb and sustain a new idea if it fits well. With these two theories, I will be able to analyze both fast and slow interactions and the way in which people adopt new technology into their lives.

The components of the network are tightly scoped to deal specifically with the user-device interaction in a home setting—the area which requires among the highest trust (Coughlan

et al., 2012). This narrow scope limits the number of connections to pull out meaningful conclusions. Technological momentum is used to investigate the overarching societal players; big companies, government, and long lasting physical hardware are slow moving entities which are resistant to change but can absorb and sustain a new idea if it fits well. With these two theories, both fast and slow interactions, along with the ways in which people adopt new technology into their lives, are analyzed. From this analysis, a framework is presented for how companies can develop Internet of Things devices in a trustworthy way and how governments can regulate those companies to protect consumers from the potential dangers of the Internet of Things.

Establishing Trust

Human trust is fundamentally built on honesty and destroyed by deceit. This duality is true of the trust between two friends and it is true of the trust a human has in a piece of technology. Openness must be a central tenet of any future where the Internet of Things is a beneficial success. Openness takes different forms in different areas of the actor-network, but underpins every recommendation. Companies producing Internet of Things devices must be transparent in the ways a device functions, what is being collected, and how data is used and stored. The more narrowly and specifically a device's functionality is defined, the easier it will be for consumers to adopt. The governments of the world can play an impactful role in the development of the Internet of things by investing immediately and heavily into public standards and open-source technologies for private companies to build on top of. This involvement, paired with input from users and entrepreneurs, will allow the drafting of legislation which gives legal backing and enforceability to some of the recommendations presented to companies.

Tim O'Reilly, founder of O'Reilly Media and one of the earliest contributors to widespread knowledge about the internet through books and guides, wrote about some of the possibilities presented by the Internet of Things in 2014:

> "My point is that when you think about the Internet of Things, you should be thinking about the complex system of interaction between humans and things, and asking yourself how sensors, cloud intelligence, and actuators (which may be other humans for now) make it possible to do things differently. It is that creativity in finding the difference that will lead to the breakthrough applications for the Internet of Things and Humans." (O'Reilly, 2014)

O'Reilly is not specifically referencing any STS framework, but the way he writes about the interaction between elements in the system resonates with Actor-Network theory in a fundamental way. In a response to that article, Kijin Sung writes: "Nothing in nature unilaterally uses anything else. It's always a two-way interaction, whether it's between a Neanderthal and his rock or between you and your self-driving car." (Sung, 2014) Although most users of technology would like to believe they lord supreme power over the devices they use, the truth is that users are simultaneously serving a function to the device or the company behind it. The web of connections which springs from the multitude of two-way interactions presents an opportunity to examine the network as a whole and find insight into improving it.

The My Friend Cayla doll is an example of an early Internet of Things device which strove to present a new use-case for the technology: children's toys. In response to a child speaking to the doll, it would convert the speech to text, search the internet for an appropriate response, then vocalize the response. My Friend Cayla was marketed as being able to converse with and entertain a child safely, but quickly became the epitome of an IoT failure when security researchers demonstrated the ability to hack the doll to act as a remote microphone and speaker. In 2017, the German Federal Network Agency issued a recommendation to parents who had

purchased the doll, suggesting that the doll was an illegal surveillance device and should be destroyed. (“German parents told to destroy ‘spy’ dolls,” 2017).

In comparison, Amazon Echo smart home speakers are prolific in the United States. Also released in 2014, the Amazon Echo is strikingly similar in functionality to the My Friend Cayla doll; users make voice queries, the Echo searches for an answer and responds with an action and/ orvoiced answer. Indeed, Amazon has faced privacy concerns of its own over the six years since launch: humans were found to be reviewing private recordings, and in a separate incident, speakers were activating without the appropriate trigger word. Why is the Amazon Echo experiencing continued success and increasing adoption while the My Friend Cayla faces destruction?

First, a distinction must be drawn between the privacy issues reported on for each device. While there are legitimate concerns about who is able to access the data from a home’s Amazon Echo, the potential bad actor in that scenario is Amazon or an Amazon employee. As a large company with experience dealing with cyber-security, Amazon has mitigated many of the security concerns which arise from having a microphone and speaker present. No significant hack has been demonstrated on an Amazon Echo which would allow third party access to the hardware or data on the device. When designing Internet of Things devices, cyber-security must be ingrained in the design process from the beginning. Tacking on security measures after the core features have been created leaves much more room for exploitation. An important difference between computer based applications and IoT devices is the presence of hardware, so this must be an additional security focus. Once an IoT device has been released, it is difficult and costly to fix or replace hardware on the device. Software patches can and should be regularly sent, but

cannot always fix a hardware-related vulnerability. In the case of the My Friend Cayla doll, a Bluetooth chip was left unsecured. The Amazon Echo has stood up to years of scrutiny and research, providing confidence to buyers and users.

The Echo has a relatively clear set of uses: playing music, ordering items off of Amazon.com, interacting with other smart home devices such as smart switches, and answering simple informational queries such as finding a sports score or reading a definition. These uses are laid out in the item description before purchase, the packaging of the Echo, and in the associated Amazon Alexa application. These prescribed uses make an Echo a useful tool. The My Friend Cayla doll failed to meet this same standard. The doll was advertised as being a conversationalist, able to have natural dialogue with children. It strove to fulfill too broad of a use case and suffered from over-generalization. How could one hand the doll to a child and know it would serve its purpose? Successful Internet of Things devices are most often designed for a specific use case. It is not possible to meet expectations without first defining what the expectations are. Many products which attempt to solve many unrelated problems end up flopping because they fail to solve any problem well. This is especially relevant in the Internet of Things where trust is built up over time.

This research is most limited by the lack of concrete recommendations in the form of specific policy proposals or technical implementation details. Rather it focuses on exploring the high-level needs of actors in the network. The Internet of Things is a continuously developing technology and field, and many of the ideas presented have not been tested rigorously. Due to that same speed of development, it is more important than ever to begin implementing best-guesses as soon as possible while remaining flexible for future changes. To future researchers, I

would most recommend interviewing stakeholders directly. Company leadership, regulatory bodies, and consumers all have unique views into the problem and could suggest new answers or new questions to answer.

Conclusion

For a company to have a successful Internet of Things device, trust must be established early and built on over time. A product must be well-defined to a specific use-case and with a full feature set presented truthfully. Security must be of the utmost concern, ingrained in the design process from day one and proven through independent security audits. The user must be able to have insight into the information being collected and control its use, and limit functionality as desired. The federal government must step in to regulate these devices to protect consumers from malicious and careless companies which may expose consumers information. Investing in these ideas now has the possibility of a safer, more productive future.

Works Cited

Ahmed, A. I. A., Ab Hamid, S. H., Gani, A., Khan, S., & Khan, M. K. (2019). Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges.

Journal of Network and Computer Applications, *145*, 102409. https://doi.org/10.1016/j.jnca.2019.102409

Ashford, R. (2014). Responsive and Emotive Wearables: Devices, Bodies, Data and Communication. *Proceedings of the 2014 ACM International Symposium on Wearable Computers: Adjunct Program*, 99–104. https://doi.org/10.1145/2641248.2642731

Ayoub, W., Samhat, A. E., Nouvel, F., Mroue, M., & Prévotet, J.-C. (2019). Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility. *IEEE Communications Surveys Tutorials*, *21*(2), 1561–1581. https://doi.org/10.1109/COMST.2018.2877382

Campbell, B., Pannuto, P., & Dutta, P. (2015, April 13). *Interfacing the internet of a trillion things*. 42–48. https://doi.org/10.1145/2756755.2756762

Coughlan, T., Brown, M., Mortier, R., Houghton, R. J., Goulden, M., & Lawson, G. (2012). Exploring Acceptance and Consequences of the Internet of Things in the Home. *2012 IEEE International Conference on Green Computing and Communications*, 148–155. https://doi.org/10.1109/GreenCom.2012.32

Danbatta, S. J., & Varol, A. (2019). Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation. *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, 1–5. https://doi.org/10.1109/ISDFS.2019.8757472

Fritsch, L., Groven, A.-K., & Schulz, T. (2012). On the Internet of Things, Trust is Relative. In R. Wichert, K. Van Laerhoven, & J. Gelissen (Eds.), *Constructing Ambient Intelligence* (Vol. 277, pp. 267–273). https://doi.org/10.1007/978-3-642-31479-7_46

German parents told to destroy “spy” dolls. (2017, February 17). *BBC News*. https://www.bbc.com/news/world-europe-39002142

Growth of Time Spent on Mobile Devices. (2015, October 7). *EMarketer*. Retrieved from https://www.emarketer.com/Article/Growth-of-Time-Spent-on-Mobile-Devices-Slows/1013072

Gudur, R. R., Blackler, A., Popovic, V., & Mahar, D. (2013). Ageing, Technology Anxiety and Intuitive Use of Complex Interfaces. In P. Kotzé, G. Marsden, G. Lindgaard, J. Wesson, & M. Winckler (Eds.), *Human-Computer Interaction – INTERACT 2013* (pp. 564–581). Springer Berlin Heidelberg.

Kabalcı, Y., & Ali, M. (2019). Emerging LPWAN Technologies for Smart Environments: An Outlook. *2019 1st*

Global Power, Energy and Communication Conference (GPECOM), 24–29. https://doi.org/10.1109/GPECOM.2019.8778626

Lo, F.-Y., & Campos, N. (2018). Blending Internet-of-Things (IoT) solutions into relationship marketing strategies. *Technological Forecasting and Social Change*, *137*, 10–18. https://doi.org/10.1016/j.techfore.2018.09.029

Montag, C., & Diefenbach, S. (2018). Towards Homo Digitalis: Important Research Issues for Psychology and the Neurosciences at the Dawn of the Internet of Things and the Digital Society. *Sustainability*, *10*(2), 415. https://doi.org/10.3390/su10020415

O'Reilly, T. (2014, August 16). *#IoTH: The Internet of Things and Humans*. O'Reilly Media. https://www.oreilly.com/radar/ioth-the-internet-of-things-and-humans/

Perry, T. (2019). The trillion-device world: ARM CEO Simon Segars says the coming 5th wave of computing is far more than a mere Internet of Things - [Spectral Lines]. *IEEE Spectrum*, *56*(1), 6–6. https://doi.org/10.1109/MSPEC.2019.8594775

Stevenson, A., & Lindberg, C. A. (2011). *Internet of things*. Retrieved from https://www.oxfordreference.com/view/10.1093/acref/9780195392883.001.0001/m_en_us1445009

Sung, K. (2014, April). *The Internet of Things: Actor-Network Theory Finally Goes Mainstream (2014)*. https://www.kijinsung.com/post/internet-of-things

Whittle, A., & Spicer, A. (2008). Is Actor Network Theory Critique? *Organization Studies*, *29*(4), 611–629. https://doi.org/10.1177/0170840607082223

Xia, H., Xiao, F., Zhang, S., Hu, C., & Cheng, X. (2019). Trustworthiness Inference Framework in the Social Internet of Things: A Context-Aware Approach. *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 838–846. https://doi.org/10.1109/INFOCOM.2019.8737491