How Attention to Transparency and Understanding User Virtues can Improve the Socio-Technical Landscape for More Private and Secure IoT Devices

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

Zachary Hogan

Fall 2022

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

Advisor
Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

> "In today's technological age someone could gain access to your online bank account through a light bulb. This is due to the Internet of Things (IoT)."
>
> -Maire O'Neill, Insecurity by Design: Today's IOT Device Security Problem, 2016

The ever-growing presence of technologies in the 21st century is remarkable for how it has facilitated the productivity of society with inventions such as smart watches, drones, and real-time video communications. However, with the advent of these technologies comes a particular set of drawbacks that pose a real danger to the public and government institutions; these dangers, though not exhaustive, include cyberattacks, the spread of misinformation, and data privacy harvesting (Tuttle, 2018). A prominent example of compromised data privacy dates back to the time of the 2016 presidential campaign when an overwhelmed public witnessed how Facebook disseminated 87 million users' information to the firm Cambridge Analytica (Tuttle, 2018). Unbeknownst to the users, their entrusted personal information was used to aid in modeling strategies to help Donald Trump secure the 2016 presidential election (Tuttle, 2018). The unsolicited disclosure and dissemination of people's private information is not a new phenomenon; there is an abundance of cyberattacks and phishing strategies that bring about a similar sense of eeriness and discomfort when it comes to privacy. As users have become more aware of the misuse of their personal information by data analytics firms and cyberattackers, user sentiment concerning privacy has been reasonably negative, especially concerning the new wave of IoT or "Internet of Things" devices (Zubiaga et al., 2018). Though people are excited about the advantages associated with IoT devices, many are increasingly concerned about breaches of trust from the misuse of their collected information (Zubiaga et al., 2018).

To resolve these privacy vulnerabilities, the underlying ethics that will be physically manifested in IoT devices must be understood. O'Neill (2016) contends the security of these

devices is paramount: “As companies race to get IoT devices to market, many are forgetting about security or all too often, security is an afterthought. Numerous attacks by IoT devices have already been demonstrated, and these attacks could have significant consequences. Therefore, companies must take the time to consider the security of their devices and include appropriate security solutions…” (p. 49). The consequences are real, deeply concerning impacts on privacy that nullify the usefulness of IoT devices. Ethics can provide a foundation by which IoT devices can be designed to safeguard user privacy and increase positive user sentiment and security, despite corporate pressures. As it stands, new IoT devices, such as smart thermostats, televisions, cameras, and toothbrushes, lack many of the encryption and data protection features that are associated with Web 2.0 products, making them more susceptible to cyberattacks and illicit monitoring (Adams, 2017). The significance of not having IoT devices that protect ethics of privacy, confidentiality, and transparency is that users may never be fully able to resolve issues of distrust with these devices. In turn, this will presumably lead users to either abstain from using the technology or never truly feel comfortable with the technology.

The purpose of this research paper is to and synthesize the ethical and technical dimensions involved in IoT design to determine what sociotechnical strategies can be employed at the user-level and the institutional-level to establish a transition to safer IoT devices. This research paper will explore the underlying question of why— if IoT devices are supposed to make life’s tasks more productive and interconnected— these devices cause public distrust and hesitancy, and how this can be ameliorated for the betterment of society. Moreover, this will include addressing IoT vulnerabilities, current user sentiment statistics, and virtues that are not emblematically present in IoT. Furthermore, evidence of how these user protections can be implemented in IoT will be explored through the use of the Multi-level Perspective Theory

framework (Geels, 2011). Effectively, the goal of this paper is to find strategies that limit users' risks and public distrust of IoT.

Problem Definition: Neglected Ethics Causing IOT Data Leaks and Unprotected Privacy

Technological Vulnerabilities Culminating in User Distrust

Infringements on digital privacy, exploitation of user information for financial incentives, and cybersecurity risks have left many people skeptical and distrustful concerning the use and incorporation of a growing number of IoT devices (Zubiaga et al., 2018). As reported by Tawalbeh et al. (2020), there are approximately 26.6 billion IoT devices used today, including domestic IoT, wearable IoT, and energy communication devices (Introduction, para. 1). Given the growth of the IoT technological sector, Yastrebova et al. (2019) report that this number of IoT devices is expected to grow to 500 billion IoT devices by the year 2030 (Internet of Things, para. 1). Based on this, the number of security incidents involving IoT is expected to increase exponentially, which not only impact significantly more users but can also have a significantly negative impact on the world economy. As shown in Figure 1, the projected IoT market is expected to reach an estimated value of 8.131 trillion US dollars by 2030 (Al-Sawari et al., 2014). To protect this growing economic sector, user protections must first be realized in order to be sustainable over the long-term.

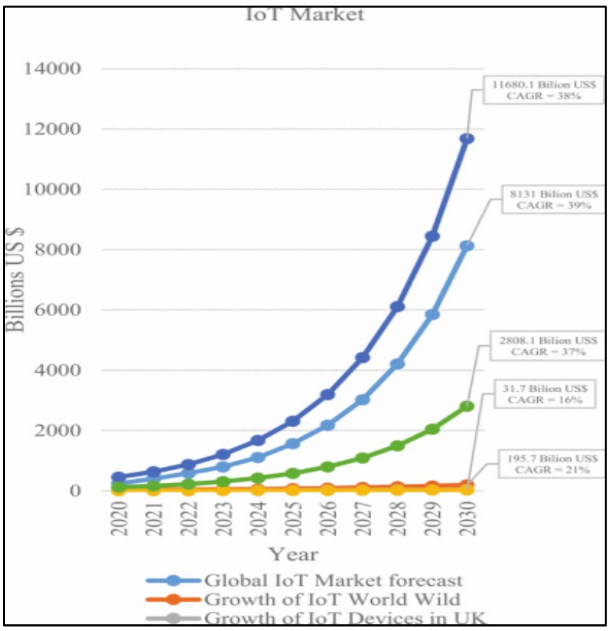

Figure 1. Estimated economics of IoT Devices ranging from the year 2020 to 2030 (Al-Sawari et al., 2014). The dark blue line indicates the market cap of the overall technological sector. The light blue line indicates the expected market cap of the IoT sector. Additionally, the green line indicates the market value of IoT in the UK exclusively. Furthermore, the yellow, red, and grey lines represent the growth in a number of IoT devices for the average device per person, the overall increase in global devices, and the increase of IoT devices in the UK respectively.

One notable ethical flaw with IoT devices is that they do not establish informed consent with the user; this concerns potential data privacy leak dangers or how to prevent these cyber-related vulnerabilities from happening in the first place. For instance, Tawalbeh et al. (2020) indicate that current IoT devices do not have features or labels that prompt users to update passwords and device software; this has been a primary vulnerability factor that has led to cyberattacks and data breaches (Security and Privacy Challenges, para. 2). Moreover, most IoT devices can flag when certain private information fields are accessed by unverified IP addresses or if private information is leaking from an unverified source (Tawalbeh et al., 2020). The very fact that the technology is capable of alerting the user but doesn't support these features is an alarming result of neglected ethics. Furthermore, Barcena & Wueest (2015) conducted a study of 50 IoT devices and reported that nearly 20% of the apps used to control these devices did not use

secure SSL connections to cloud storage (Key Findings, para. 1). Additionally, none of these devices in the study provided any mutual authentication between host and server connections, leaving them especially vulnerable to cyberattacks (Key Findings, para. 1). This indicates the insufficient application of ethics in technologically capable IoT devices. Moreover, these vulnerabilities have led to severe consequences on public morale and user trust.

With these known vulnerabilities, users of IoT have become increasingly wary of whether or not these technologies promote the users' safety and privacy (Walker, 2016). According to a study by the Pew Research Center, 68% of adult users believe that United States laws do not offer sufficient protections for data leaks of personal and private information involving internet-related activity (Walker, 2016). Moreover, 75% of IoT users polled do not believe that manufacturers are not incorporating adequate security technologies in IoT devices, and 73% concluded that industry standards offer limited user protections (Loughran, 2015). Based on a study conducted by Emami-Naeini et al. (2019), security cameras and other IoT video-recording devices have gathered the greatest statistical measurement of user distrust (with $p < 0.05$) (p. 9). Video monitoring attacks are especially disturbing given the extent to which they can violate user privacy. This includes documented attacks on vulnerable IoT baby monitoring systems where baby footage has been rerouted and viewed by attackers (Lastdrager et al., 2020). Moreover, IoT-related violations of user privacy have not gone unnoticed as sentiment analysis on Twitter suggests in Figure 2.

Growing Negative User Sentiment

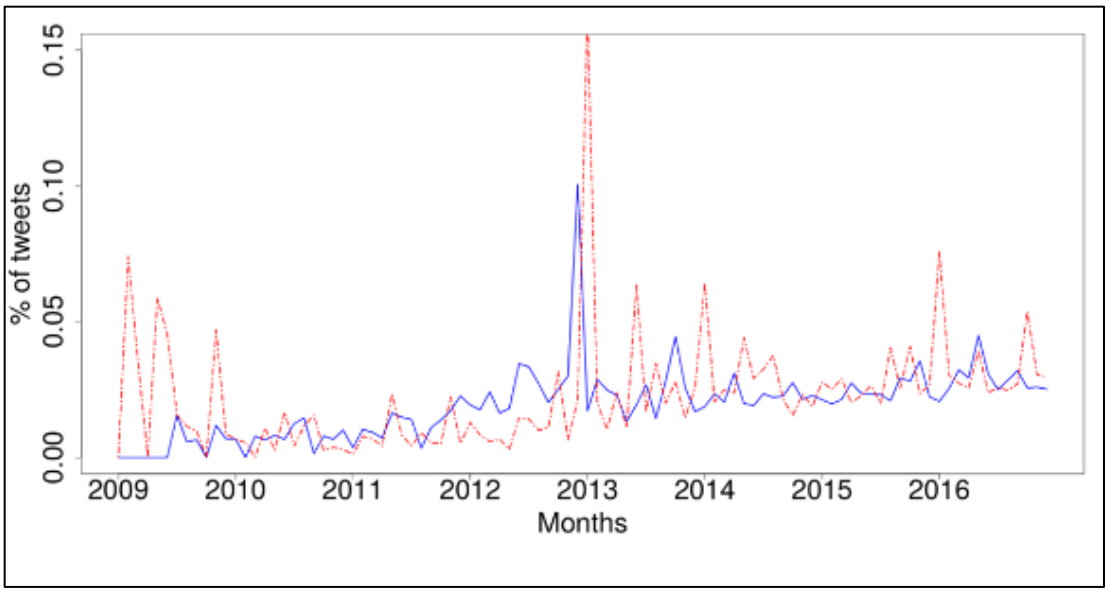

Figure 2. Sentiment measurements were obtained from Twitter Tweets regarding IOT devices (Zubiaga et al., 2018). This graph ranges from the year 2009 to 2016 with positive sentiment indicated by the blue line and negative sentiment indicated by the red line.

As shown in Figure 2, sentiment analysis of IoT security in Twitter Tweets illustrates that negative sentiment has increased by 15.09% from 2009 to 2016 (Zubiaga et al., 2018). This trend is important to note because as IoT devices become increasingly popular in the technological sector, the associated vulnerabilities have noticeably increased as well. Without addressing these vulnerabilities, negative sentiment will only increase over time. This is highly significant because this may continue to give IoT devices a negative connotation and may potentially lead to users abstaining from using them altogether. As illustrated in Figure 3 below, these statistics are moreover affirmed by a survey that found 40% of users fear that their private health information will be exploited and that 63% of users fear their IoT devices are susceptible to hackers (Loughran, 2015).

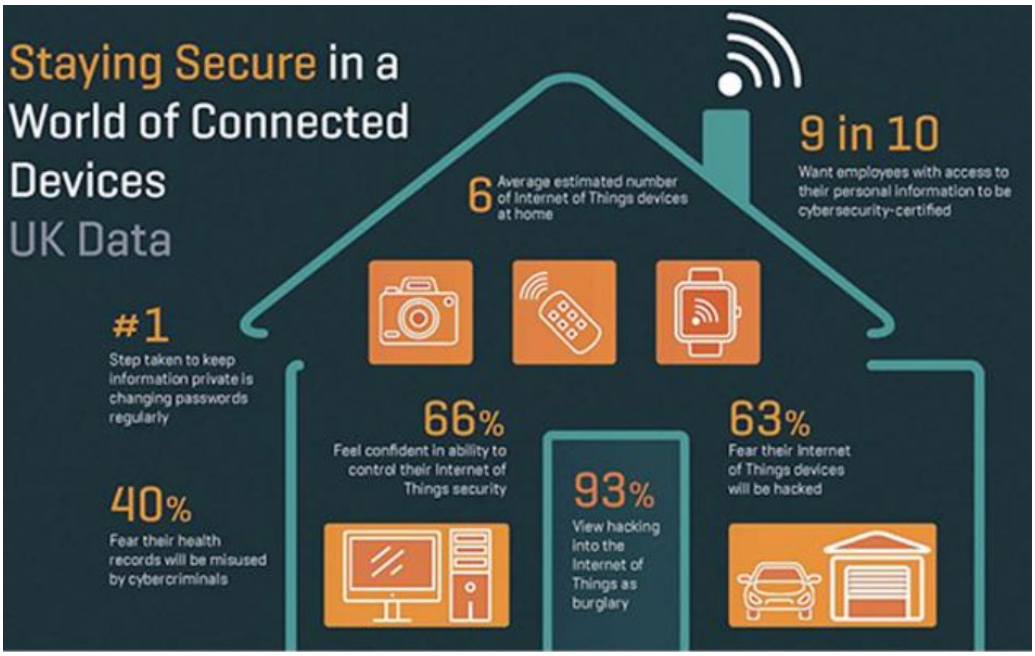

Figure 3. A survey indicated common user concerns about IoT devices (Loughran, 2015). This infographic concludes that a majority of users are concerned about IoT privacy as well as IoT cyberattacks which 93% view as an act of burglary.

Remedying negative IoT device sentiment so that users can regain a sense of control over the dissemination of their private information is difficult without proper encryption. For instance, health and other sensitive information require extra care in data transmission to ensure that only the intended recipient should receive it, or if it should even be sent at all. Potential solutions to these problems are promising but not yet conclusive. Kotagi and Moriai (n.d.) contend that, since IoT is designed to operate on low power, it is often not well-equipped with the ability to encrypt data communications, and, thus, non-traditional cryptographic processes should be considered such as light-weight cryptography (p. 3). Additionally, despite IoT's computational limitations, Barcena & Wueest (2015) assert there is no excuse for a lack of encryption:

> IoT devices often have less memory and slower CPUs, so they may be unable to use the same encryption methods as a traditional computer does, but this is no excuse for the lack of strong encryption. There are efficient cryptographic methods designed for small-scale

devices, such as Elliptic Curve Cryptography (ECC), which can be used (Conclusion, para. 1).

The need and importance— for the sake of privacy— to engineer cryptographic algorithms compatible with IoT devices reflects the necessity to not forego privacy protections for the sake of expanding the IoT network and increasing revenue. Neglecting this ubiquitous safety issue will only exacerbate the problem and leave users feeling unsafe and sketpical.

Improving positive IoT sentiment and trust expands beyond not only enhancing the physical security of the devices but also the enacting of societal values and concerns. As aforementioned, a significant percentage of users fear that their private information will be accessed by IoT cyberattacks (Loughran, 2015). What is unknown is how to tackle these persistently unresolved IoT vulnerabilities through a cultural lens by focusing on user-defined ethics. By recognizing the need to incorporate ethics involving transparency, privacy, and safety into IoT devices, real changes can potentially be made over time to ensure that IoT devices align with users' values as illustrated by the Multi-level Perspective Theory (Geels, 2011).

Part II: Applying principles of the Multi-Level Perspective (MLP) Theory to Model Socio-Technical Transitions in IoT

MLP as a Framework to Understand the Evolution of Technology

The negative societal impression that IoT devices have left on topics such as safety and privacy appears to be growing over time as discussed regarding Twitter sentiment (Zubiaga et al., 2018) and polls conducted by the Pew Research Center (Walker, 2016). However, this trend does not have to continue if certain actions are taken to reaffirm trust with users. Actions can be

taken at the legislative level or the user level to advocate for physical values in the technologies to improve user comfort. Of course, reversing this negative sentiment will take time, but there is one framework that shows promise in reverting to more ethical practices of IoT: the Multi-level Perspective Theory (MLP) (Geels, 2011).

Applying principles of the Multi-Level Perspective (MLP) Theory helps to model sociotechnical transitions that technologies have historically undergone to predict future transitions. As Geels (2011) illustrated, there are key aspects of the model to understand a sociotechnical transition from an older practice to a newer one (p. 28). In a sociotechnical system, three parties constitute the main entities of technological change: the socio-technical regime, the socio-technical landscape, and the niche (p. 28). Geels (2011) describes the socio-technical regime as the existing policies, corporations, and government entities that support a fixed application of technology (p. 27). Along with this higher stratum dictating the rules by which the technology should abide, there is the niche, which can be summarized as the users or disruptive researchers who introduce transformative ideas on how the technology can best be used differently (p. 27). This may include innovative actors, research facilities, or groups of users who do not feel the technology encompasses their needs (p. 27). Lastly, the socio-technical landscape represents a region, nation, or other domain for the use of technology (p. 28).

To apply MLP to reveal how technologies can change to the needs of society progressively over time, it is important to understand how the new ideas of the niche embody values that are not fully represented in technologies established by the socio-technical regime. The misrepresentation of societal values in technology brings about a cultural pressure of constructive change to the overall socio-technical landscape (p. 29). Users and other actors see

that the current regime either adopts technologies whose implementations are harmful and over time pushes technologies and practices that would better suit society's needs.

In a slow progression, the accumulative research, user suggestions, and evolution of the ideas of the niche begin to be reflected in the socio-technical landscape. As these suggestions begin to pick up momentum, the once originally non-commonplace ideas of the niche gradually become the more commonly adopted practices of the socio-technical regime (p. 26). Geels reveals the efficacy of this framework in the context of the present-day transition from non-renewable energy to sustainable energy (p. 25). From a sustainable energy perspective, Geels (2011) shows how corporations and policies have sustained large oil corporations that have been historically lucrative business models; however, as users and researchers have come to realize, these practices of the socio-technical regime are inherently destructive to the environment and hazardous to people's health (p. 25). As people have begun to raise their voices in favor of a new sustainable system, technologies and favorable practices have followed: clean fuels, windmill generators, and non-gasoline vehicles. An overview is shown in the figure below, which summarizes the stages of a general MLP transition (Geels, 2011).

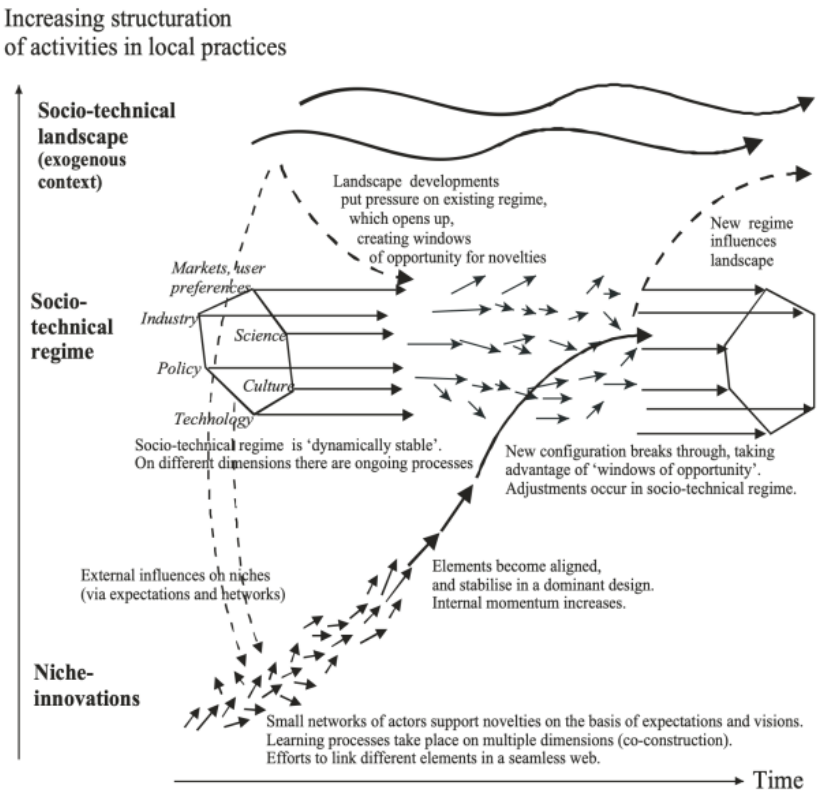

Figure 2. Interactivity and influence over time among the three primary entities of the Multi-level Perspective Theory: The Socio-technical Landscape, the Socio-technical Regime, and the Niche (Geels, 2011). As time progresses, the socio-regime shifts to meet the demands of the socio-technical niche.

The MLP Theory is relevant to the research of this paper because it demonstrates how the evolution of new, niche ideas and technological practices gain momentum to replace previous technological practices that were not as well-suited to the needs of society. With regards to the IoT landscape, niche, and regime, these entities correspond to corporate practices, users, and corporations as well as government institutions, respectively. These bodies are always evolving to meet the greater need, and, as such, the 'norm' of IoT cannot remain constant. Though Geels (2011) represents MLP Theory in the context of a transition to sustainability, MLP Theory can be equally as useful in understanding how vulnerable, insecure data practices involving IoT devices do not have to be commonplace. MLP Theory can reveal how the impact of personal

data leaked by corporations as well as IoT device cyber vulnerabilities can be made safer by society. By introducing new practices from research and activist groups, the socio-technical regime can be altered to allow for safer data protections and practices to be reflected in the socio-technical landscape.

Part III: Results and Inferences of Evidence for Safe IoT

Ethical Engineering Practice in IoT

When considering the many concerns and lack of protections of IoT, the first line of defense I consider is the engineer and the engineer's ethical toolkit. As discussed earlier, IoT devices are highly sophisticated and interactive devices that communicate information with other wireless access points across the world. Though IoT devices serve a very mechanical and technological purpose, they also constitute human values anywhere from the design stage to distribution. An engineer has biases and values that become intertwined with the technology's purpose. If an engineer is aware that an IoT design is susceptible to cyberattacks, the lack of informing customers of this flaw is nothing but blatant dishonesty. For instance, as Tawalbeh et al. (2020) suggested, many of these IoT devices which have known defects in their architectures make no effort in informing the user of the potential security ramifications of when a default password is not reset (Future of the Internet of Things, para. 7). As indicated by Hosseini et al., (2016) this lack of transparency is neglected in most IoT designs, though it is paramount to user safety:

> Transparency is advocated to inspire trust, increase accountability, and reduce corruption… Despite its distinct characteristics and importance, transparency is still a

> limitedly explored concept in software engineering and information systems literature and is often fragmented across adjacent concepts such as privacy, secrecy, and regulatory requirements (p. 225).

From a business standpoint, it is understandable that broadcasting a product's weaknesses in tandem with its strengths may make the product look more unattractive. However, the impact of a lack of informed consent and transparency in these devices may prove to be more detrimental as users are unaware of the ramifications until after a breach has occurred.

It is the responsibility of engineers to not dismiss ethics in the creation of IoT, despite corporate or monetary pressures. When the technology's features are in alignment with the engineer's ethics, the physical protections, including efforts for increased encryption, software updates, and limited port access by greedy third parties, will naturally follow suit. Though this will not make IoT technology invincible to cyber threats, the ethics instilled in the hardware will presumably grant greater user comfort. Moreover, this evidence suggests that transparency, honesty, and confidentiality are indispensable to an engineer in augmenting positive user sentiment and decreasing abuse of private user information.

Different Outlook on Multi-level Perspective Theory for Ethical IoT

One of the most self-evident aspects of the transition to safer IoT devices is knowing its place regarding the Multi-level Perspective (MLP) Theory product cycle. As public sentiment becomes increasingly negative, the demand for products that adhere to the values and needs of users increases. As shown in Figure 2, negative public perception has only increased over the years from 2009 to 2017, thus indicating a lack of modifications with IoT that enhance security

features and practices (Zubiaga et al., 2018). This lack of change in sentiment suggests an ongoing struggle between user interests and those of the socio-technical regime; furthermore, it appears that the regime may be resistant to enact these changes. Over time, I predict that negative sentiment regarding IoT will only increase as users feel that their values are not reflected in their own IoT devices.

Based on the observation that IoT sentiment has not changed for the better, users may be playing an ineffective game of tug-of-war with the corporations and policies that may be inclined to believe they have no real incentive to place additional safeguards on user data. Unlike an MLP cycle for products that enhance user physical safety, the adverse effect of compromised digital security is more elusive. For instance, the socio-technical creation of automobile seatbelts is more readily understood to be needed to prevent physical harm; however, the harm caused by data privacy leaks may be perceived as less urgent as there may be no immediate danger or knowledge that this digital harm is even happening to the user. Therefore, navigating security IoT improvements is most likely a relatively new application of MLP, and dictating desired changes to the socio-technical landscape may prove to be more difficult by using traditional approaches than with products with physical ramifications.

Relevant Entities that could Facilitate Change in IoT

Given the technical complexity of IoT and the expensive resources required to fabricate these devices, there are most likely only a very small number of niche actors that can present alternative technologies and policies that conform to public interests. One powerful set of actors could be researchers and professors at universities as their research can influence a wide network of academic audiences. In addition to standards that fit electrical and computational standards,

publications can begin to develop protocols that conform to user safety and marketing strategies can be implemented to promote informed consent. As these protocols begin to be adopted by institutions such as IEEE, the industry standards would begin to follow suit; thus, this could facilitate MLP on behalf of users.

In addition to rewriting standards on the behalf of user safety, another angle to tackle this problem could be through lobbyists and activists to impact policy directly. A potential decision-maker who may support the results is the Electronic Frontier Foundation (EEF) which advocates for digital privacy. This organization places emphasis on the freedoms and rights of users that should be respected regarding technology use, including IoT communications (Budington, 2022). Given that they present to conferences to reveal systemic issues with technological practice, they may use these ideas to advocate for safer IoT, which could bring about changes in corporate practice as well as government legislation. The EEF's reputation and efforts could serve as a conduit to enable corporate and legislative bodies to understand how a lack of user protections in IoT is causing real harm to users. Furthermore, this would expedite changes in the IoT socio-technical landscape as users now have a voice in promoting changes that safeguard their privacy and right to safe technologies.

Conclusion

Unsafe IoT devices and practices have been resistant to change in alignment with the values of users. From Twitter sentiment analysis to polls, statistics indicate a growing net-negative sentiment towards these devices in not safeguarding privacy and protections against data leaks (Zubiaga et al., 2018) (Walker, 2016). Furthermore, the lack of transparency in device vulnerabilities and the lack of informed consent involving data harvesting appear to be the main

drivers of these sentiments (Tawalbeh et al., 2020). However, this negative trend does not have to be a constant; the Multi-level Perspective Theory shows how users, policymakers, and corporations interact to evolve the applications of technologies to best serve the ethical needs of users over time. If engineers embody ethics— including honesty, transparency, and accountability— in their technological pursuits and account for the needs of the user base, positive changes in the socio-technical landscape can occur for everyone's benefit if additional measures are taken to make digital harm a serious legislative matter.

For the sociotechnical landscape to adjust to the needs of users, there has to be an impetus that starts with the users and organization to implement changes within corporations and governments. IoT device applications and security features can be modified to best fit the needs of users in several aspects. The first starts at the IoT design phase with the engineer and company culture upholding security and privacy to a high standard. Since this appears to have been neglected as of present concerning IoT, the user base can change the way IoT serves their needs through research, legislation, and policy. Through the work of activist groups and organizations such as the EEF, representatives of these groups can advocate for changes in upholding security and data privacy measures on behalf of users. Though a gradual process, policy, and standards can serve as an effective means to improve user sentiment regarding IoT, accommodate user comfort, and build trust.

References

Adams, M. (2017, April). Big Data and individual privacy in the age of the internet of things. Technology Innovation Management Review. Retrieved September 18, 2022, from https://timreview.ca/article/1067

Al-Sawari, S., Anbar, M., Abdullah, R., & Hawari, A. (2014). Internet of things market analysis forecasts, 2020–2030. IEEE Xplore. Retrieved October 20, 2022, from https://ieeexplore.ieee.org/abstract/document/9210375

Barcena, M., & Wueest, C. (2015, March 12). Connecting everything. Broadcom Inc. Retrieved October 16, 2022, from https://docs.broadcom.com/docs/insecurity-in-the-internet-of-things-en

Budington, B. (2022, July 13). Keeping your smart home secure & private. Electronic Frontier Foundation. Retrieved October 27, 2022, from https://www.eff.org/deeplinks/2022/06/keeping-your-smart-home-secure-private

Emami-Naeini, P., Dixon, H., Agarwal, Y., & Cranor, L. F. (2019, May 4). Exploring how privacy and security factor into ... - ACM Digital Library. Retrieved September 19, 2022, from https://dl.acm.org/doi/pdf/10.1145/3290605.3300764 [Journal article]

Geels, F. W. (2011, February 26). The multi-level perspective on sustainability transitions: Responses to seven criticisms. Environmental Innovation and Societal Transitions. Retrieved September 18, 2022, from https://www.sciencedirect.com/science/article/abs/pii/S2210422411000050

Hosseini, M., Shahri, A., Phalp, K., & Ali, R. (2016). Foundations for Transparency Requirements Engineering. Retrieved October 20, 2022, from https://www.researchgate.net/publication/298721124_Foundations_for_Transparency_Requirements_Engineering

Katagi, M., & Moriai, S. (n.d.). Lightweight cryptography for the internet of things. Retrieved September 19, 2022, from https://iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf

Lastdrager, E., Hesselman, C., Jansen, J., & Davids, M. (2020). Protecting home networks from insecure IOT devices. IEEE Xplore. Retrieved October 12, 2022, from https://ieeexplore.ieee.org/abstract/document/9110419

Lee, H., & Kobsa, A. (2016). Understanding user privacy in Internet of Things environments. IEEE Xplore. Retrieved September 18, 2022, from https://ieeexplore.ieee.org/abstract/document/7845392

Loughran, J. (2015, October 14). Security vulnerabilities plague IOT devices survey finds. RSS. Retrieved October 16, 2022, from https://eandt.theiet.org/content/articles/2015/10/security-vulnerabilities-plague-iot-devices-survey-finds/

O'Neill, M. (2016). Insecurity by design: Today's IOT device security problem - researchgate. Retrieved October 28, 2022, from https://www.researchgate.net/publication/301827951_Insecurity_by_Design_Today's_IoT_Device_Security_Problem

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020, June 15). IOT privacy and security: Challenges and solutions. MDPI. Retrieved September 18, 2022, from https://www.mdpi.com/2076-3417/10/12/4102/htm

Walker, K. (2016, April 1). Surrendering information through the looking Glass ... - sage journals. Retrieved September 19, 2022, from https://journals.sagepub.com/doi/10.1509/jppm.15.020

Yastrebova, A., Kiricheck, R., Koucheryavy, Y., Borodin, A., & Koucheryavy, A. (2019, February 3). Future networks 2030: Architecture & Requirements. IEEE Xplore. Retrieved October 16, 2022, from https://ieeexplore.ieee.org/abstract/document/8631208

Zubiaga, A., Procter, R., & Maple, C. (2018, December 20). A longitudinal analysis of the public perception of the opportunities and challenges of the internet of things. PLOS ONE. Retrieved September 18, 2022, from https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0209472#pone-0209472-g001