A Game of Fog and Mirrors: Privacy in the World of Internet of Things

Alice F. Parker[1], Tor-Morten Grønli[1] and Muhammad Younas[2]

[1] Mobile Technology Lab, Department of Information Technology,
Kristiania University College, Norway
[2] School of Engineering, Computing and Mathematics,
Oxford Brookes University, Oxford, United Kingdom

Abstract. Privacy challenges are a growing point of research in both political science and computer science as the pervasive nature of IoT devices turns Orwell's dystopic state into a potential reality. This research maps out potential scenarios for IoT privacy challenges in the interdisciplinary effort to understand what it means to have privacy in world of internet-enabled sensors.

Keywords: Internet of Things, information security, privacy

1 Introduction

One of the greatest challenges facing both technology and politics in the 21st Century is coming together in spearhead, and that spearhead is IoT and ubiquitous computing. Privacy is not a new challenge to either paradigm. This is a research area that started centuries ago. Neither is it a research area that is likely to be solved anytime soon. Yet the pervasive nature of IoT is demanding that the 'balance of privacy' craves an interdisciplinary effort as the two paradigms collide. This research will map out the road leading up to this intersection, as well as visualise the challenges of IoT privacy in both technological and political disciplines.

IoT's boom in recent years has seen it commonplace for internet-enabled devices in homes, transports, and streets around the world. Already, are there almost as many sensors as humans, and soon sensors will be numbered in trillions. [1] As Weiser predicted, these sensors are "so ubiquitous that no one will notice their presence." [2] Each and every heartbeat and breath taken can be recorded and the data sent into the cloud and out of the control of the individual. Their footsteps, geolocation, smile, and speech are amongst the various things that can be tracked through these ubiquitous sensors placed in our watches, mobiles, fridges and even our ski boots. [3] Whilst the technology is still in its infancy, it is not ridiculous to perceive that one day a sensor in human brains will be able to send bio signal data to into the hands of others. Literally reading our thoughts. Regardless of the current unfeasibility of brain-computer interaction, advancements in AI means that with the data presently available we can already create models to predict what humans may do next. Before they have thought of it themselves.

1.1 Privacy versus Confidentiality

As a newcomer to privacy in data protect and IoT, it seems as if the researchers from political paradigms like cybersecurity policy and international politics, and the researchers from human-computer interaction and technology, are sitting in the same room with their backs to each other and demand that they talk face to face, yet neither turns. A common way to start a dialogue is to begin with the same language. For that, definitions on key terms need to be established. Privacy is the first definition to agree upon. For a system to protect user privacy, one needs to know what privacy is. The OED definition of privacy is:
"The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion." [4] The European Union's legal interpretation is in the form of General Data Protection Regulation (GDPR) which came into force in 2018. The law, whilst only European, applies to all European citizens wherever they are in the world. GDPR "asks you to make a good faith effort to give people the means to control how their data is used and who has access to it." [5] It is important to note that this is already a break from the common definition of privacy, as it does not necessarily imply one is free from interference or intrusion. An IoT device is GDPR compliant when ensuring that it is transparent with the user about their data and the purpose for keeping it, as well as facilitating a simple way for the user to control where their data is, the IoT device is GDPR compliant. This does not necessarily corelate to privacy. It may be closer to the interpretation of confidentiality. Nor does GDPR protect users for unfaithful actors or define how to implement the law in a technological sense. Neither, does it calm qualms for users with inherent distrust of the law and state.

1.2 Privacy in philosophy mirrored in IoT

A debate on the morality of the state will not dominate this research, but it is important to acknowledge the ambiguity and subjective nature of the IoT privacy actors. The discussion on privacy can be traced back to the 18th Century, if not further. Jeremy Bentham, a British political philosopher, devised the Panopticon as a way in for prison guards to easily see all prisoners from one spot, without moving. [6] His argument was that a prisoner, never quite knowing if the guard was watching, would behave and this was to their own benefit. We can draw strong lines between this prison architecture and IoT's ubiquity. The user is never easily aware of when sensors are present. [7] In this sense, individuals are prisoners, captive to the IoT device prison guards.

A century later the French philosopher, Michel Foucault, highlighted the cruel societal ramifications of the Panopticon state. Whilst the thought that an omniscient government might have benefits of both deterring and catching those who act outside the law, regardless of whether the omniscience is presumed or genuine, this leads to dynamic normalisation. [8] IoT devices have already appeared in the media as heroes in criminal cases, such as home assistant devices keeping evidence of premeditated murder. [9] In a tyranny this directly facilitates the eradication of freewill, for example the

persecutions of minorities or other groups seen as a threat to the survival of the tyrannic state. Even in a democracy, Foucault argues, can also have fundamental consequences on independent thinking and creativity. Thus, leading to the erosion of democracy. [8]

If one needs any more elaboration on the dystopic nature that could be entailed with IoT, one only needs to draw upon George Orwell's 1984. [10] The difference between his fictious writing and present day is that the technology is far more ubiquitous than Orwell's imagination allowed. IoT is the technology that turns his fiction into theoretical possibility. It is very important to note that at no point is the morality of privacy invasion assessed. This research give an objective overview of privacy invasion regardless of the justifications.

1.3 Privacy versus Security

Cybersecurity is a large research area. It can often take priority over privacy research. It is necessary to distinguish the difference between security and privacy. Alwarafy et al. cover the security and privacy threats to Edge IoT but do not distinguish between the two, nor do they look at what these threats to mean outside boundaries of IoT. [11] The dystopian trajectories illuded about above do not make an obvious case for a threat to security. A scenario where society ends up like Orwell's 1984 is often not considered in cybersecurity. Privacy violations are precursory to security violations and their security implications may not be directly obvious. The privacy violation of the US citizens' Facebook data by Cambridge Analytica was not a threat to security on an individual scale, nor was it a threat to national security until it allowed a small elite to effectively control the outcome of a supposedly democratic election. Cybersecurity research will cover data theft, but research into privacy needs to consider when this data is given either lawfully or with consent. There is an intrinsic link between security and privacy, yet the consequences of IoT privacy breaches warrant their own research in a setting where they are considered a precursor to security threats at both national and personal levels.

2 Methodology

The brief overview of the political and philosophical discussion on privacy makes it evident that Orwellian invasions of privacy can be mirrored and played out through IoT research. This paper follows design science methodology by presenting a map of scenario variables in IoT privacy threats and placing existing research on IoT privacy solutions within this map. The interdisciplinary nature of the subject means research from both political science and technology will be applied. It is important to note that in political science paradigms, the theories of realism, liberalism and critical theory are continuing to throw differing results and predictions. The political science paradigms are used to back up the privacy implications but the theories will not be used to assess the technological nature of the article.

What follows is a literature review of an assortment of different research articles that tackle the challenges in IoT privacy from different perspectives. The backgrounds of the researchers in these articles span across nations (from the US, UK and to China) and research area (legal, political, and computer science).

Following this, we will present the map of IoT privacy scenario variables and ensue in a discussion on the prior literature in relation to produced artefact.

3 Literature Review

3.1 Who's Afraid of the Big Bad Smart Fridge?

Tanczer et al. [12] amply set the scene to a world in which IoT security and privacy threats are left unchecked. Their "future and foresight methodologies allow for the exploration of plausible futures and their desirability." They were able to categorise these areas in 4 common themes: (1) Physical safety, (2) Crime and exploitation, (3) Loss of control, (4) Social norms and structures. [12] By identifying and discussing potential dystopian scenarios, the hope is for IoT researchers to better strategize and tackle issues of IoT privacy and security. An example provided is "The seamless tracking of car users through companies that build and operate such smart cars may also lead to further erosions of privacy and individual's autonomy and sense of autonomy." [12] Their work very much highlights the trajectory of IoT left unchecked. In a world in which "we give up freedom for convenience", they conclude on two opposing possible outcomes. The first is that mass hysteria and public outcry will force the individuals to shun IoT technology regardless of whether the benefits of their use outweigh the perceived privacy threats. The second is a scenario in which society is complacent, passive and apathetic to privacy invasions. Tanczer et al's [12] research also shows that IoT researchers are currently pessimistic that proposed frameworks to govern IoT privacy and security will result in compliance and enforcement measures from the manufacturers of IoT devices. Neither is "keeping out an unauthorised actor through access controls and erecting barriers such as firewalls, is unlikely to remain effective." [12] Finally, Tanczer et al [12] articulate that privacy issues in societal discussion are continuously ongoing, IoT entering this debate will only complicate the issues further. Their article presents a depressing trajectory for IoT which allows researchers to focus on important points to address in future research. Left out is the discussion of 'good' and 'bad' privacy invasion, and the mapping of actors causing the privacy invasion.

3.2 The Cloud, the Private Sector and the State

Pre-GDPR, Macropoulos et al's [13] IEEE opinion article explores the dangers to an individual's privacy where the state is the main threat. "The private sector has a pivotal role to play in balancing the privacy needs of the individual and the security demands of the state." [13] Their article illustrates the role that the private sector places in an individual's right to privacy. Not only for the benefit of the individual, but in a scenario

where “customers believe their privacy is under threat, their choice of provide will be heavily biased by trust considerations,” [13] and the company itself is in jeopardy. Whilst not focusing directly on IoT, but instead at general cloud computing prior to the widespread adoption of edge comping and the implementation of GDPR, the article raises contributions about the location and control of data. A combination of “political, legal and technological approaches” is needed to address the issue. Macropoulos et al, echoing Tanczer et al, state that “information technology is merely the newest arena within which societies are seeking to balance the needs of the state with the expectations individuals.” [13] The contribution this article plays is the perspective of there being more than one actor portrayed as the victim of privacy invasion and more than one actor portrayed as the perpetrator.

3.3 GDPR Compliant User-Centric Privacy Frameworks

GDPR is considered the most far reaching and powerful laws made on data protection in world history. “GDPR aims to give control of personal data back to the user.” [14] Kounoudes et al. propose GDPR-compliant framework for IoT devices. Rather than looking at privacy as a challenge to overcome, they look at providing privacy protocols in a user-centric way “without blocking the evolution of IoT.” [14] They map existing frameworks to GDPR characteristics and look at solutions. Their three main contributions to IoT privacy mechanisms are as follows:

- Machine Learning techniques have been thoroughly used to provide user privacy protection.

- Using policy languages to specify user privacy preferences and to express complicated policies. - Optimising the trade-off between privacy and utility. [14]

3.4 Privacy by Design

“Privacy must be addressed not just in terms of static regulatory requirements but also in terms of developing best practices for IoT industry”. [15] As a neglected aspect in the design of IoT, “an understanding of data movement is focal to ensure accurate and complete threat location, system analysis and compliance assessment.” [15] Thorburn et al look at the methodologies and guidelines needed to ensure IoT privacy compliance. These they categorise into six points:

- Data flow
- IoT Privacy Taxonomy
- Privacy-by-Design Focus
- Audit
- Implementation
- Compliance and risk driven [15]

The significance of the privacy-by-design frameworks are covered in the discussion below.

3.5 Conceptual Privacy Frameworks

Chow creates a conceptual privacy stack framework for a IoT user-centric privacy protectionism. [7] This privacy stack builds on ensuring the control of data is in the hands of the user and enabling the user to customise data flow based on their own preferences. The unique and ubiquitous nature of IoT calls for a more attentive approach to data protection. Visualised in Fig. 1, IoT designs should consider the awareness, inference, preferences and notification that users have when it comes to their data. "A basic privacy principle is that personal data collection should happen only with appropriate notice and choice." [7] The aim is to build a channel of communication between the IoT provider and the user for preserving the individual's privacy.

3.6 Privacy Mediators

To fulfil demands for user data control, Davies et al. [16] present cloudlets. Cloudlets, a privacy mediator, act as a secure and independent gateway between the IoT device – be it a chip or a system of IoT devices, and the cloud provider or company. The user is in complete control over what information is sent. This is "a scalable and secure solution on the edge of the cloud." [16] Data is kept local and close to the device rather than being streamed through a vast distributed system. Not only does this protect the user from the technology provider, but also from outside cyber-attacks as the data's surface area is now reduced.

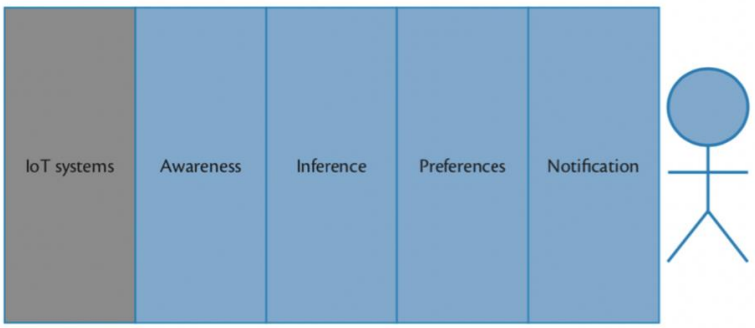

Figure 1 The privacy stack framework bridges from today's Internet of Things (IoT) systems to users. [7]

This architectural framework provides the user with a "rich set of privacy controls." [16] Mediators can be placed at varying degree of granularity and provided by 3rd party providers, much like anti-virus software today, and can be controlled in context-aware setting. Davies et al also play close attention to detail on video data processing, memory

storage location and privacy control settings. The data would be “logically within the trust domain of the end user,” [16] state, situating the cloudlets at the edge of the cloud.

3.7 Local Differential Privacy in Edge Computing

Unlike the previous articles shared that have explored giving the control to user’s about where their data ends up, Bi et al. [17] propose a more cautious solution that takes into consideration the dishonest and the ‘honest-but-curious’ third parties that may deliberately or inadvertently leak private data. The authors of the paper focus purely on location data. Bi et al. [17] remark on the similarities between blockchain and edge computing decentralised technology as beneficiary to protecting user’s privacy. However, blockchain is still too burdening for processing at the edge to be widely used in IoT. Bi et al. [17] use local differential privacy as method for prevent data collection centres from ever getting users’ accurate location data. Local Differential Policy “transfer the privacy process of data to each user, enabling users to individually process and protect personal sensitive information.” [17].

3.8 Federated Learning

A similar model for ensuring as little data as possible strays far from the user is proposed by McMahan et al. at Google [18]. Their model also promotes lower latency and energy consumption. Using a miniature version of TensorFlow, machine learning algorithms can process data and create outputs without the input data being sent to the central cloud. Only the aggregated data is ever sent back to the cloud. This technology is just one example of how designers are pushing more and more of the architecture to the edge of the cloud, and closer to the user [18].

4 Discussion

To understand the challenges for IoT in terms of privacy threats, we need to map out all the surface area. Fig. 2 shows the variables that can be in play without depicting the relationship between each group. This is not necessarily a comprehensive summary of the different variable elements, but the point is to demonstrate that in order to discuss privacy in IoT, we cannot have a one size-fits-all solution. It is often assumed that the victim of IoT privacy invasion is an individual that either has access to the IoT device itself or access to privacy settings through their mobile device. But there is little consideration that the victim might be an individual that has no knowledge or access to the IoT device or privacy settings. The victim may also be a group of people or a state, which would involve the use of aggregated data rather than specific raw data.

The aggressor, the one inflicting the invasion of privacy, can also be categorised into different groups. The finger is often pointed towards “honest-but-curious third parties”

[17] as the violators of privacy. However, a more nuanced approach into the flow of data and why the data is needed. There is also no value in looking at one of the end nodes of the map in Fig.2 in isolation, we must build a scenario in which the end nodes are used in combination. Fig. 3 shows all the possible ways in which Bob can have his privacy violated: either an indirect threat (the violation of his privacy through aggregated data) or a direct threat (where the violation of Bob's privacy can be traced directly back to him). It is important to illustrate the different relationships between the victim and the aggressor as these will indicate at what point the privacy is invaded.

The scenarios illustrated above are not imagined, we can find examples of these expressed in the media. Recent concerns were raised about employee privacy when Amazon vans installed video cameras to make their drivers take rest breaks if the technology determines the driver is tired [19].

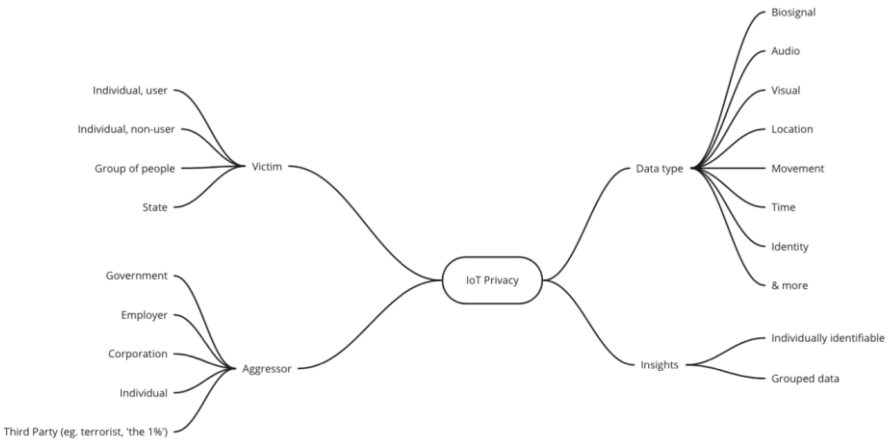

Figure 2 IoT Privacy Scenario Variables.

Affective computing means emotions are no longer private from Orwellian surveillance. Scenario 2 and 3 demonstrate this in Fig. 3. Carlo, highlights that the "constant monitoring of employees creates an oppressive, distrustful and disempowering work environment that completely undermines workers' rights." [19].

By mapping the threats to Bob's privacy, we can begin to look at where the gaps are in research to address privacy issues in IoT. Tanczer et al [12] take a similar approach, by calling upon leading IoT experts to express their trajectories of IoT left unchecked. Many of the violations to Bob's privacy at an aggregated level are mentioned in Tanczer et al.'s research. [12] Scenarios marked in green in Fig.3 show scenarios where privacy could be violated from aggregated data. "We give up freedom for convenience." [12]

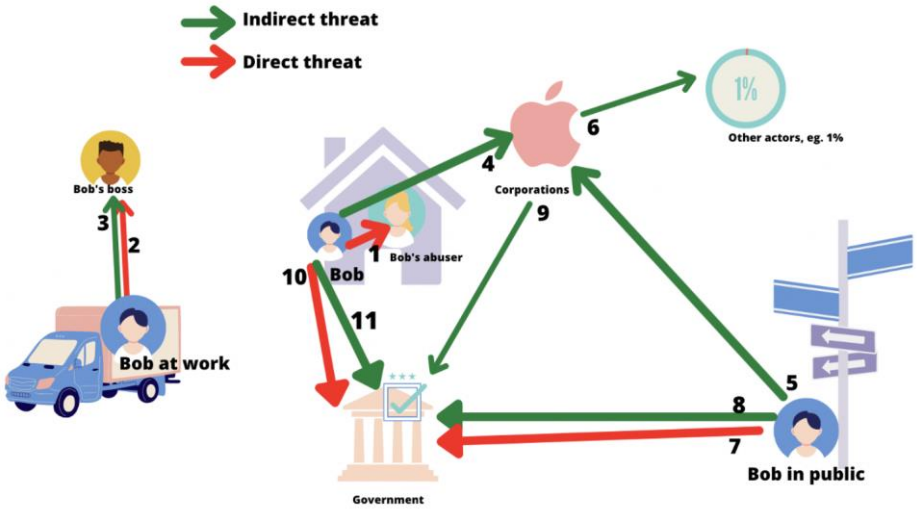

Figure 3 Privacy Scenario Map with the individual (Bob) as a victim

Frameworks allow a breakdown of concepts and making it easier to think through concepts when designing and assessing risk. The research for GDPR compliant frameworks in Kounoudes et al. maps their identified challenges to GDPR characteristics, as shown in Fig 4. Similar to the research from Chow, (private by design) and Davies et al. [16], the privacy preserving mechanisms are reliant on the user being able to make informed decisions about the usage of their data. They both make effort to ensure that services "explicitly provide basic inferences." [7]. There is a considerable amount of privacy preferences research not mentioned in this research that look into enabling users to make empowered privacy preference choices. Tanczer et al's research lay challenge to this as one trajectory for IoT privacy challenges is apathy. "Individuals would consequently lack suitable alternatives that provide them with the opportunity to freely give consent and remain in control over how their data is being collected and processed." [12] No number of choices or power over their own data is sufficient when the user does not care what happens with their data.

Mapping of GDPR characteristics to challenges

	Characteristic	CH1	CH2	CH3	CH4
CR1	Prevent inference	√			
CR2	Provide data transformation	√		√	
CR3	Provide user awareness on data collection				√
CR4	Provide control of personal data to users		√	√	
CR5	Provide monitoring and control of devices that collect data			√	
CR6	Provide tools for data management to users		√	√	√
CR7	Provide ability for data erasure		√		
CR8	Provide transparency		√		√
CR9	Provide balance of privacy between users and third parties		√		
CR10	Provide enforcement of user privacy preferences			√	
CR11	Provide privacy by design or privacy by default			√	
CR12	Provide ability to users to make informed consent choices			√	
CR13	Estimate privacy risks of data collection/inference to users			√	
CR14	Communicate risks of data collection/inference to users			√	
CR15	Provide ability to users to specify their privacy preferences			√	
CR16	Prevent excessive data collection			√	

√= subject addressed; (blank) = not addressed

Figure 4 Mapping of GDPR characteristics to challenges [16]

Bi et al. [17] take the more cautious route by assuming all data centers are untrustworthy. Whilst not explicitly referred to, McMahan et al [18] also provides the same solution. Data leaving the edge nodes is aggregated and the user's individual privacy is left undisturbed. Fig 5 from Bi et al. [17] shows how the raw location data never leaves the client's devices. These solutions also allow for the value of the data being sent back to the central cloud not to be weakened. Federated Learning sends the trained dataset back to the shared model. [18]

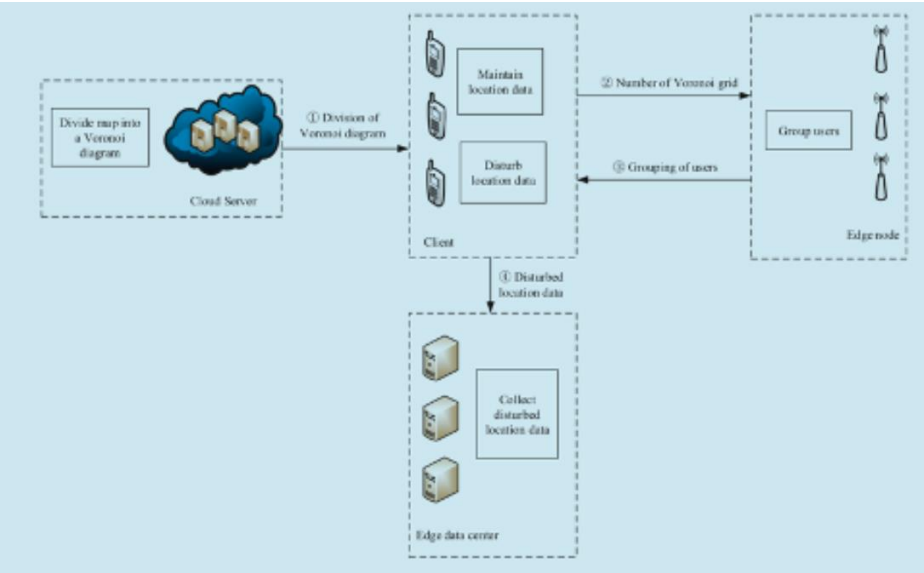

Figure 5 Bi et al. Voronoi Privacy Preserving Method

Edge computing has become a popular architectural structure for IoT devices due to its lower latency and keeping the user's data closer to the edge of the network. Additionally, research often uses self-built and self-controlled IoT hubs to sync and manage

the interoperability of numerous devices. Consumers opt for commercial IoT hubs such as Google Nest or Amazon Echo which ultimately allow the devices manufacture access to all data flowing through these devices. Understanding that the lawful passing of data as illustrated in scenarios marked in green are central to the concerns raised by Tanczer et al. [12]

Finally, neither current privacy control preferences nor privacy preserving mechanisms within IoT gateways and even GDPR compliant frameworks can protect Bob's privacy from an abusive individual with legal access to IoT devices that monitor his movements. Fig 3. shows this in scenario 1. This is a scenario that Tanczer and Parkin et al. [20] research. The surface area for privacy threat from a domestic abuser is all encompassing as visualised in Fig. 6. Their research is still in the infancy to be able to provide contributable solutions, but they indicate fair usability is an essential part of the design stage in IoT devices. This is something that the research in the literature reviews that create privacy-by-design frameworks for IoT devices does not cover.

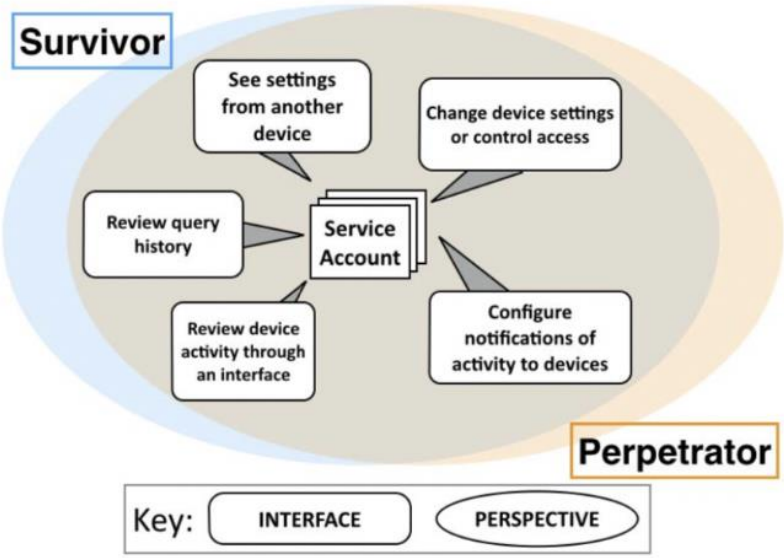

Figure 6 Perspectives and interfaces onto a service account in a climate of tech-abuse. [20]

5 Limitations

There are several limitations in the contributed map and table to lay out the challenges that face IoT privacy. Firstly, and most significantly, the mapping ought to be

applied to all major IoT privacy research. There is also a need for stronger research into the privacy violations using aggregated data. This is mentioned in Tanczer et al. [12]'s research on the trajectories of IoT privacy challenges but there is a need to look at it from a purely technical perspective. Whilst this research distinguishes the privacy violation scenario differences from corporation, third party and government aggressors, there requires more attention to the differences of these actors. This is would be similar to the work of [13] yet calls for research specific to IoT devices in a GDPR world. The scenarios listed also only focus on individuals as a victim and it would be useful to look at the scenarios where businesses and states are the victim. Finally, there this is a need for more refined policy on privacy challenges when the data is obtained with informed consent, permission and on an aggregated level.

6 Conclusion

In order for IoT privacy challenge research to thoroughly address weaknesses and understand the potential threats to individual and grouped privacy, we need to begin with a map of the scenarios possible. This calls for an interdisciplinary effort from both political science and computer science researchers. Tanczer et al's [12] research shows a promising start to the collaborative work required.

As laid out in the introduction, privacy has been researched for centuries. IoT merely moves this into a new paradigm and complicates the matter further. [13] By acknowledging the unfinished and contentious nature of privacy in philosophical spheres, it prevents naivety of IoT technology researchers to preclude that a simple privacy mediator or mechanism may suffice.

To reiterate, this research does not attempt to label any scenario of privacy violation as justified or not. The first step is to recognise where the privacy is invaded, and then leave it to philosophers and policy makers to decide on the rational. Following this, technology researchers can then implement the desired frameworks for enabling Private-by-design IoT devices. Frameworks covered in the literature review do make a start on privacy-by-design, but the map produced in Fig. 4 shows that not all the scenarios have been designed for. Edge Computing has facilitated more privacy for the end user, but it still leaves many scenarios unchecked.

If not anything, the mapping of the multitude of threats, victims and scenarios in IoT privacy challenges shows that this is truly a game of Fog and mirrors.

7 References

1. Chetan Sharma, “Iot data privacy framework,” http://www.chetansharma.com/publications/iot-data-privacy-framework/, accessed: 2021-02-09.
2. M. Weiser, “Ubiquitous computing,” Computer, vol. 26, no. 10, p. 71–72, Oct. 1993. [Online]. Available: https://doi.org/10.1109/2.237456
3. Carv, “Carv,” https://getcarv.com/, accessed: 2021-02-07.
4. Oxford University Press, “privacy, n.” https://www.oed.com/view/Entry/151596?redirectedFrom=privacy, accessed: 2021-02-11.
5. European Union, “Gdpr data privacy,” https://gdpr.eu/data-privacy/, accessed: 2021-02-11.
6. J. Bentham and M. Bozovic, The Panopticon writings. London ; New York: Verso, 1995.
7. R. Chow, “The last mile for iot privacy,” IEEE Security Privacy, vol. 15, no. 6, pp. 73–76, 2017.
8. M. Foucault, Discipline And Punish : the Birth of the Prison. New York: Pantheon Books, 1977.
9. Privacy International, “Timeline iot in court,” https://privacyinternational.org/timelineiotincourt, accessed: 2021-02-12.
10. G. Orwell, 1984, centennial. ed. Tandem Library, 1950.
11. A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, “A survey on security and privacy issues in edge computing-assisted internet of things,” IEEE Internet of Things Journal, pp. 1–1, 2020.
12. L. M. Tanczer, I. Steenmans, M. Elsden, J. Blackstock, and M. Carr, “Emerging risks in the iot ecosystem: Who’s afraid of the big bad smart fridge?” in Living in the Internet of Things: Cybersecurity of the IoT - 2018, 2018, pp. 1–9.
13. C. Macropoulos and K. M. Martin, “Balancing privacy and surveillance in the cloud,” IEEE Cloud Computing, vol. 2, no. 4, pp. 14–21, 2015.
14. A. D. Kounoudes and G. M. Kapitsaki, “A mapping of iot user-centric privacy preserving approaches to the gdpr,” Internet of Things, vol. 11, p. 100179, 2020.
15. R. Thorburn, A. Margheri, and F. Paci, “Towards an integrated privacy protection framework for iot: Contextualising regulatory requirements with industry best practices,” in Living in the Internet of Things (IoT 2019), 2019, pp. 1–6.
16. N. Davies, N. Taft, M. Satyanarayanan, S. Clinch, and B. Amos, “Privacy mediators: Helping iot cross the chasm,” in Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, ser. HotMobile ’16. New York, NY, USA: Association for Computing Machinery, 2016, p. 39–44. [Online]. Available: https://doi.org/10.1145/2873587.2873600
17. M. Bi, Y. Wang, Z. Cai, and X. Tong, “A privacy-preserving mechanism based on local differential privacy in edge computing,” China Communications, vol. 17, no. 9, pp. 50–65, 2020.
18. McMahan, Brendan and Ramage, Daniel, “Federated learning,” https://ai.googleblog.com/2017/04/federated-learning-collaborative.html, accessed: 2021-02-09.
19. Wakefield, Jane, “Bbc | amazon faces spying claims over ai cameras in vans,” https://www.bbc.com/news/technology-55938494, accessed: 2021-02-04.
20. 21. S. Parkin, T. Patel, I. Lopez-Neira, and L. Tanczer, “Usability analysis of shared device ecosystem security: Informing support for survivors of iot-facilitated tech-abuse,” in Proceedings of the New Security Paradigms Workshop, ser. NSPW ’19. New York, NY, USA: Association for Computing Machinery, 2019, p. 1–15. [Online]. Available: https://doi.org/10.1145/3368860.3368861