Knowing and Not Knowing:

The Problem of Privacy in

an Internet-of-Things World.

Submitted in Partial Fulfilment of the Requirements for the Bachelor of Media and Communications (Honours).

Matt Adair, s3204584, Bachelor of Design (Multimedia Systems)

Supervised by Thomas Penney, RMIT, Lecturer - Industry Fellow (Digital Media)

2016

/*

* Compiled – 11th October 2016

*/

/*----------*

I certify that except where due acknowledgement has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the thesis is the result of the work which has been carried out since the official research program; and any editorial work, paid or unpaid carried out by a third party is acknowledged.

----------/

/*----------*

Acknowledgements:

Thomas Penney for supervision, advice and the necessary encouragement.

Dr. Adrian Miles for providing RMIT Media & Comm. Honours support and advice.

Mira for absolutely everything.

Mum for proofreading and everything.

MH4U for just being there.

----------/

Image: Smart phone under the light of the Internet-of-Things (All images in this thesis are of the author’s project).

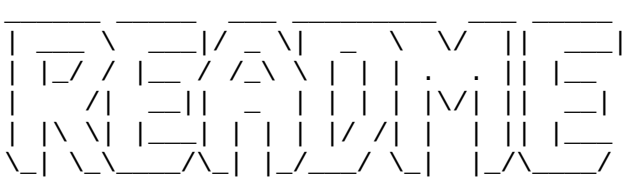
TABLE OF CONTENTS

/**********/

ABSTRACT

/**/

In the context of the emerging Internet-of-Things (henceforth known as IoT) our relation to technology is changing as the IoT is embedded within seemingly unrelated objects. The IoT suggests a new paradigm in which individuals are submitted to the range of its sensors; we are offered no choice but to surrender to its monitoring. Through Critical Engineering I will investigate a technique currently being deployed by technology companies that allows an IoT device to communicate with a smart phone in a manner hidden from the phone's user. This gives rise to urgent social and political concerns surrounding privacy and identity issues, particularly given that the impetus for the propagation of the IoT is the identification and tracking of people by both governmental and commercial organisations. The extraction of personally identifying information as we pass through the range of the IoT is particularly insidious when these organisations use this data to make decisions that can dramatically affect our lives. I hope to make people aware of this through the reading of this text, project and code.



/***

*

* supporting materials and locations

* archival copies of the following resources are available via the attached media.

*

***/

CFP_Ultra Android application code repository:

// Java source files and compiled binaries

https://github.com/kaputnikGo/CFP_Ultra

Project website:

// HTML 5, CSS and JavaScript

http://akm.net.au/pilfershush/index.html

Demonstration video:

// online video player

https://vimeo.com/183291077

INTRODUCTION

/**/

The central aim of this honours thesis and project is to investigate specific technological implementations that give rise to privacy concerns. To do so, this thesis will examine the inaudible audio communication between an internet-of-things (IoT) device and a smart phone based on a Critical Engineering[1] project. The IoT device is capable of audio playback at frequencies considered to be beyond the typical range of human hearing when the audio signal is at low amplitude.[2] In the same way that Morse code transmits intelligence as a series of audio tones representing letters of the alphabet, near ultra-high audio frequencies can serve a similar function. This research uses the IoT device as the transmitter of discrete tones that represent a form of intelligence and uses the smart phone as the decoder of these signals.

Within this investigation I define and identify the capabilities of a specific type of IoT for broadcasting audio and the necessary smart phone hardware and software to receive the audio. To demonstrate the phenomenon this thesis will refer to a Critical Engineering project element that consists of a smart phone application with open source code[3], an IoT enabled light bulb and a film[4] that records the interaction between the two. The choice, construction and interaction of these elements will be discussed in detail later in this thesis.

While this thesis investigates hardware and software that may prove too complex to accurately describe here, it is the intention to investigate the fundamentals of IoT audio technology in order to

1 "The Critical Engineering Manifesto," Julian Oliver et al., published 2011, https://criticalengineering.org.
2 S. Smith, "Audio Processing." in *The Scientist and Engineer's Guide to Digital Signal Processing* (San Diego,: California Technical Publishing, 1997), 353.
3 "Android near ultra-high frequency listener," kaputnikGo, GitHub Inc, published 18 Aug. 2016, https://github.com/kaputnikGo/CFP_Ultra.
4 "PilferShush-demo-01-proper," Vimeo video, 03:30, posted by s3204584, accessed 30 Sept. 2016, https://vimeo.com/183291077.

concentrate on possible interactions and examine their potential meaning and repercussions. Technology research is often based upon a specific technology that will either become obsolete, redundant or even non-existent after a period of time. With this in mind, this research is based on a specific implementation of the IoT in order to discern how its specificities shape its function and ultimately reveal how this technology can affect the user in ways not immediately apparent. One of the questions arising from this research is whether the ability of the IoT to communicate with our phones without our awareness is a cause for cultural, social or political concern. Do we have a "trustworthiness among devices and users"?[5]

// Internet-of-Things

The IoT is the term used to describe a type of machine-to-machine technology that consists of computer chips, sensors and an internet connection[6]. They can be embedded within everyday objects and enable an emergent ambient intelligence capability[7]. Alternatively they can be stand-alone beacons placed in locations as diverse as bushland and urban shopping centres. These sensors may be used to do things as simple as measuring rainfall over periods of time, or to record and track movements through a particular area[8].

For the purpose of this research IoT devices will be defined as technologically unique not only in their capabilities but, because of their small size, allowing "themselves to vanish into the background"[9]. These hidden devices and their associated networked processing systems are designed to perform so that together "they can anticipate human needs based on information collected about their context"[10]. This crude understanding of the IoT provides a basis for an

5 Sabrina Sicari et al., "Security, Privacy and Trust in Internet of Things: The Road Ahead." *Computer Networks* 76 (2015): 160.
6 Lara Srivastava et al., *The Internet of Things*. Geneva: International Telecommunications Union, 2005: 1.
7 Salvatore Gaglio and Giuseppe Lo Re, eds., *Advances onto the Internet of Things*. Advances in Intelligent Systems and Computing, Vol. 260. (Cham: Springer International Publishing, 2014), 33.
8 Srivastava, *The Internet of Things*, 21.
9 Mark Weiser, "The Computer for the 21st Century." *Scientific American*, Sept. 1991, 94.
10 Srivastava, *The Internet of Things*, 21.

investigation into how such devices can communicate with smart phones. The study of key audio communication processes and the software development techniques involved will be the basis for a reflection on problems of privacy within the context of technologically mediated communications.

The use of IoT devices has been referred to via marketing names such as the Physical Web or beacons[11]. This marketing maintains that the digital web can be present in the physical world by giving any item that can house such a small IoT device the means to connect it to the internet[12]. For example a pair of shoes for sale in a shop could have a small IoT beacon inside them that transmits a link to the web page for those particular shoes. When a shopper is within a certain distance of the shoes their smart phone may receive notification that announces the shoes' presence and transmits the link for a website.

This process currently relies on the Bluetooth radio and protocols that exist in most smart phones. While the Bluetooth radio essentially relies on the same radio frequencies and methods of transmission that have been used since its invention, the software layer has evolved, rendering device version compatibility a concern for vendors of this technology. For instance, one of the latest additions to the Bluetooth protocol allows for the broadcast of a hashed URL (e.g. 0x08 0x0008 1a 02 01 06 03 03 aa fe 12 16 aa fe 10 00 00 61 6b 6d 0a 2e 61 75 2f 69 6d 6c 2f 00 00 00 00 00) via Bluetooth low energy transmissions (BTLE). The broadcast has a range of approximately 10 metres radius from the beacon and is easily readable by any phone with the required software.

The successful receipt of this broadcast requires that, at the very least, the Bluetooth radio is turned on and the user has allowed the Bluetooth radio to receive transmissions from unknown (un-paired) devices. This requirement has meant that a sizeable proportion of shoppers will not be able to

11 "The Physical Web," Google GitHub repository, accessed 28 Sept. 2016, https://google.github.io/physical-web/.
12 Australian Communications and Media Authority. *The Internet of Things and ACMA's areas of focus*. (Canberra: Australian Communications and Media Authority, 2015), 5.

receive these notifications due to either BTLE software incompatibility or because they have their phone’s Bluetooth switched off. Lack of connection via Bluetooth has created a desire on the part of the vendors to reach these shoppers via alternative methods prompting the development of near ultra-high frequency audio beacons.

These audio beacons communicate the same type of messages via sound waves at a frequency higher than can be heard by a human but within the range of a typical microphone. This use of audio transmission is favourable for the vendors as it is more likely to be received. The majority of smart phones have functioning built-in microphones: this method therefore bypasses the problem of establishing a connection when relying on a given smart phone's Bluetooth compatibility and whether the Bluetooth is turned on.

// Smart phones

Apart from the IoT device that emits inaudible signals we require a smart phone and its ability to receive and decode such signals. The ever-expanding role a smart phone plays in collective life will not be discussed here; suffice to say that it may be the singular and central item that a person uses for many of their social interactions. The user also retains a level of control over these devices, made visible via the device settings which allow the user to determine when, how and in what manner their device can communicate. The control the user can exercise over their device also plays a significant role in this research, which will be examined in the later discussion.

The mobile phone has come a long way since Motorola first released its hand-held analogue cellular model in the early 1980s. Mobile phones are referred to as smart phones due to the addition of small computing components that allow the user to perform actions much as they would on a desktop or laptop computer. In order to do so the smartphone consists of an operating system (OS) that not

only enables phone calls but also provides an Application Programming Interface (API), allowing anyone with the necessary skills to write their own executable software for the phone.

Referred to as third-party software, this is limited in its interactions with the fundamental hardware layer by the methods and functions that are presented to the programmer via this API. For instance, the OS may have a function that allows a third-party application (app) to connect to the internet via the cellular network. A requirement for this may be that the third-party app needs to notify the user of the smartphone that this connection is about to occur. It may even give the user the ability to override this action and inform the OS that no connection is allowed to be made.

As part of this research project I have created an app that mimics the functions of commercial ones already available in the market place. The techniques employed by the app are neither limited to one brand of smart phone or one brand of operating system nor are they robust to production level standards. However, they do provide a means to examine the phenomenon discussed in this thesis centred on inaudible audio communication between the IoT and smart phone.

// Critical Engineering Project

The investigation into this phenomenon is made using the methodology of Critical Engineering that seeks to study and expose the inner workings of a technology. The Critical Engineering Manifesto declares that it is the role of the engineer to closely examine the technology that surrounds us and shapes the way a society functions. Through a close examination of the specifics of implementation the engineer is able to ascertain the functional realities and subsequent effects that may not be visible to the casual observer either due to complexity or designed obfuscation[13].

13 “The Critical Engineering Manifesto,” Julian Oliver et al., published 2011, https://criticalengineering.org.

There are some moments of cross-over between this methodology and what has variously been referred to as the Maker movement, or Critical Making, with its “emphasis on critique and expression”[14]. However, these methods tend to be limited to do-it-yourself craft in which the maker is primarily concerned with what they can create rather than the broader social implications of that creation. The Critical Engineering method is primarily concerned with revealing and determining any effects that may arise for a society and its technology. The purpose of undertaking a project in such a manner is to ask the audience to critically engage with the way we interact with a given technological implementation[15].

To demonstrate and understand IoT to smart phone communication this research will create a contrived use-case scenario that will consist of the key hardware and software elements. These elements will be placed within a stable environment suitable for observing an IoT device transmitting near ultra-high audio signals to a smart phone. The smart phone will be running open source software that can decode this signal as a set of instructions and then execute secondary processes based upon those instructions.. A simple user interface will be used to demonstrate a degree of information about what is occurring at any time during the application’s execution.

This scenario is designed to demonstrate that it is possible to directly communicate between an IoT device and a smart phone without the user’s knowledge. This communication, in turn, causes processes to take place in the background of that device, also without the user’s awareness. This interaction will be measured by reference to a film that records a demonstration of the completed use-case scenario. A fuller description of the examination of the software and hardware that facilitates this will be discussed in the following sections.

14 Matt Ratto, “Critical Making: Conceptual and Material Studies in Technology and Social Life.” *The Information Society* 27, 4 (2011): 253.

15 “The Critical Engineering Manifesto,” Julian Oliver et al., published 2011, https://criticalengineering.org.

THEORETICAL CONTEXT

/**/

//Contextual Introduction

One of the earliest investigations into the phenomenon of inaudible audio signals being transmitted to mobile phones was published in an article on the Ars Technica website[16]. The article informed the reader about privacy concerns being raised by the Center for Democracy and Technology[17] who filed comments to the US Federal Trade Commission regarding several companies pursuing a particular type of Cross Device Tracking (CDT). CDT allows website vendors to follow a particular user as they switch between different devices[18]. This submission made to the FTC took place on October 16th 2015 and it was not until March 17th 2016[19] that the FTC responded with a warning letter sent to unspecified developers that may have included a Software Development Kit (SDK) in their code that performs the audio listening, recording and processing functions.

While the IoT may present itself as a new and disruptive industry[20] it is merely an extension of preceding technologies that either offer a means to communicate or insert themselves in the middle of human social interactions. My research will uncover the act whereby hidden IoT devices communicate with a person's private property, the smart phone. Taking the smart phone beyond the personal use for social interactions, the IoT can communicate with the user's phone and can initiate an internet data connection, or push advertising via the Physical Web. It can also, by simply

16 "Beware of ads that use inaudible sound to link your phone, TV, tablet, and PC," Dan Goodin, Condé Nast, published 14 Nov. 2015, http://arstechnica.com/tech-policy/2015/11/beware-of-ads-that-use-inaudible-sound-to-link-your-phone-tv-tablet-and-pc/.

17 "Cross-Device Tracking Requires Strong Privacy and Security Standards," Katie McInnis, Center for Democracy & Technology, published 19 Oct. 2015, https://cdt.org/blog/cross-device-tracking-requires-strong-privacy-and-security-standards/.

18 Roberto Dıaz-Moralesl, "Cross-Device Tracking: Matching Devices and Cookies." *2015 IEEE International Conference on Data Mining Workshop* (2015): 1699.

19 "FTC Issues Warning Letters to App Developers Using 'Silverpush' Code," Kristin Cohen, Federal Trade Commission, published 17 Mar. 2016, https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code.

20 Australian Communications and Media Authority. *The Internet of Things and ACMA's areas of focus*. (Canberra: Australian Communications and Media Authority, 2015), 5.

initiating a connection, profile the user via information gleaned from the device to the extent made possible by the smart phone operating system.

The theoretical impetus for this thesis is: does this unannounced and uncontrollable communication from an IoT device to our smart phone constitute a privacy concern? Does the potential for a hidden transmission of personally identifying information represent a privacy violation? Media and Communication theorists have long wrestled with the impact of the rapid development of technology, both on the individual and on society as a whole.

// Theory

The implications of expanding internet-based technologies for privacy and their impact on traditional legal, political and cultural assumptions, is one of the central problems of this research. While the internet and the role of privacy within it are not new concepts, privacy has become more prevalent with the expansion of social media and could be considered one of the defining problems of our age. What were once understood to be the user's private life and thoughts, are now published on various privately-owned corporate internet platforms such as Facebook, Twitter, Instagram, etc. As a result there is a growing awareness of potential privacy concerns within the area of social media expressed in academic research, journalistic investigation and commentary. Several of the key ideas dedicated to this problem are investigated here.

These analyses tend to contextualise the problem domain in relation to its historical precedents. Such responses to privacy concerns are not new nor are they simply a collection of obscure ideas favoured only by academics, as any glance at news or current affairs media can attest. The notion that privacy is a site of contest is not limited to the contemporary context, in which private companies mediate social interactions via the internet; it necessarily underpins all forms of

communication. These approaches also include investigations into responses that have arisen when any new technology or technique is adopted on a large scale, from the first email exchange to the latest tweet.

However, "deeper origins can be found... when one realises that technology need not mean computing nor be digital"[21]. Re-examining social theories from pre-internet era media is useful only as a reminder that, regardless of technological changes and "the notion that everything is new"[22], there are some fundamentals at play when people interact with technologically mediated communications. Debates around these questions have seen the theoretical expansion and evolution of "issues about the quality of interaction, the nature of community, the status of relationships, the authenticity of identity, the safety of children, and the limits of trust and privacy"[23].

Theorists have explored not only what effects are produced but also what changes are made to the way we communicate when technology is the intermediary. These are issues that arise when "people simultaneously integrate multiple media into their daily communicative experience" which serves to "cut across once-familiar boundaries separating mass from interpersonal"[24]. The intersection described here results in the dissolution of traditional boundaries between private and public, singular and mass and ultimately gives rise to new problems around the question of privacy.

The problem of privacy can also arise when technologically mediated socialising takes place "within proprietary systems", which rely on "users' unpaid labour to generate their content"[25]. Concerns around the use and purpose of these systems also raise questions about behavioural

21 Nancy K. Baym, “A Call for Grounding in the Face of Blurred Boundaries.” *Journal of Computer-Mediated Communication* 14, 3 (2009): 720.
22 Ibid.
23 Ibid.
24 Ibid., 721.
25 Ibid., 722.

responses: what happens when we acknowledge that we do not have complete control over the aspects of our lives we imagine to be private?

An assumption of the late twentieth century was that the physical and digital worlds are distinct. However, recent thinking and analysis suggests that the idea of a person existing online as a separate and anonymous version of the real-world analogue "is outdated and has largely been abandoned"[26]. In the early days of the internet it was thought that an online identity was something "that was easily put on and taken off while the Internet guaranteed anonymity"[27]. Today we imagine these two identities to be interchangeable and the anonymity once provided can no longer be guaranteed.

The merging of digital and analogue identities, while "not functionally equivalent", do combine in such a way that they "co-create the experience of identity"[28]. The influence of one over the other is apparent when we consider that these two sides of identity are so closely entwined. When we transform "our private subjectivity into public content"[29] we are in some ways presenting our private analogue self as the digital public self, a relationship that can operate in both directions. This can be understood as a "feedback loop, a dialectic" between our public and private selves in which "one domain informs the other"[30].

The ideas of public opinion formation via internet-based mass media and the integration of our digital and analogue selves can be used to describe the current information technology environment. We can augment this description if we consider that this environment also "alters our sense of time

26 J. Sage Elwell, “The Transmediated Self: Life between the Digital and the Analog.” *Convergence: The International Journal of Research into New Media Technologies* 20, 2 (2014): 233.
27 Ibid., 234.
28 Ibid., 235.
29 Ibid., 237.
30 Ibid.

and space, and we adapt to these changes"[31] even if they provide us with "ersatz experiences upon which opinion rests"[32]. Despite this desultory appraisal there is a strong undercurrent of a "technological utopianism"[33] that drives society to adopt and utilise the various internet-connected media devices in the belief that it "insures our collective survival and success" via the "the consumption of goods and services"[34]. This phenomenon that produces an "overload of information" generated by digital media "transforms us into consumers of information"[35].

The digitising of the self, and the accompanying reduction of identity to internet-rendered data, has meant that "people become visible, knowable, and shareable in a new way"[36]. The theory known as "surveillance capitalism" demonstrates that it is now possible to "predict and modify"[37] as well as "observe behaviour that was previously unobservable and write contracts on it"[38]. This is enacted at the corporate level through "incursion[s] into undefended private territory until resistance is encountered"[39]. This process has been described as "infrastructure imperialism"[40]. The companies in the vanguard of this development describe what they do as an "extractive process" that occurs in the "absence of dialogue or consent"[41]. Its application reveals that information is extracted "without consumers' knowledge, consent, or rights of privacy"[42]. It also reveals one of the most pernicious aspects of a technological infringement of privacy that takes place when we are not aware of its occurrence.

31 Richard Stivers, “The Media Creates Us in Its Image.” *Bulletin of Science, Technology & Society* 32, 3 (2012): 203.
32 Ibid., 206.
33 Ibid., 207.
34 Ibid., 208.
35 Ibid., 209.
36 Shoshana Zuboff, “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization.” *Journal of Information Technology* 30, 1 (2015): 77.
37 Ibid.
38 Ibid., 81.
39 Ibid., 78.
40 Ibid.
41 Ibid., 79.
42 Ibid., 78.

In a technological society consisting of a "ubiquitous networked institutional regime that records, modifies, and commodifies everyday experience" control resides with a "sovereign power"[43] that can "reconfigure the structure of power, conformity, and resistance"[44] via its control over the digital realm. In response to concerns around privacy rights and violations, corporations argue that "people agree to the invasion of privacy" required for these companies to exist "if they get something they want in return"[45]. Given the popularity of social media, and other internet services based on the voluntary surrender of personal information, it would appear that this is the case. An alternative way of framing this concept might be to understand that the intention "is not to erode privacy rights but rather redistribute them"[46]. A redistribution can occur between the individual and the corporation when the latter has "extensive privacy rights and therefore many opportunities for secrets" while the former is deprived of "choice in the matter of what about their lives remains secret"[47].

The corporate control over the medium of communication operates via mechanisms such as intellectual property laws, corporate laws, proprietary software and patented technologies. When corporations deploy new communication technologies or techniques they demonstrate that "rapid abilities to surveil for profit outrun public understanding"[48]. The communication surveillance taking place now is merely a precursor to a future in which a corporation will "know what you want and tell you before you ask the question"[49]. To do so, at the data and algorithmic level, it "has to know a lot about you and your environment to provide these services"[50]. The provision of this information is achieved by data generated by a technology "that is also regarded by most people as essential for

43 Ibid., 81.
44 Ibid., 82.
45 Ibid.
46 Ibid., 83.
47 Ibid.
48 Ibid.
49 Ibid.
50 Ibid.

basic social participation"[51]. Somewhere in this lies the concept of privacy, the right to privacy and normative behaviour that seems to offer tacit approval for privacy violations.

// Incorporate

The concept of privacy still exists when the typical smart phone user wishing to install an app is made aware of the vendor's privacy policy and any app permissions required. Even without reading and fully comprehending these statements their existence alone indicates the continued legal, social and cultural relevance of the concept of privacy. What this Critical Engineering project seeks to demonstrate is that such a basic level of awareness is not possible when certain features, such as listening for inaudible audio, are hidden from the smart phone user by design. It is also not possible for the smart phone user to be aware that there is an IoT device hidden, also by design, somewhere within their surrounding environment.

By creating a scenario to explore such a phenomenon, this research will promote thinking about the differing levels of privacy and control over information by publishing and utilising techniques hidden from casual observation. Technical abilities submerged in complexity or deliberately hidden by the vendor are presented in a manner that brings several of their effects to the foreground. When observing these effects, such as an IoT device doing something that causes the smart phone to load a browser web page, we may be able to consider this ability in differing contexts and for differing purposes. However, primarily we need to understand that this occurred without any user interaction or control.

The broader context described here by media and communication theory relates not only to how we interact but also to the technological medium itself, which has an ability to influence this interaction. This influence takes place in an asymmetrical manner: we know who we are

51 Ibid.

communicating with and yet there is an opaque third party in between that surveils and responds to who we are and what we are saying. Technological capabilities aside, what is most relevant here is that a corporately owned medium has its own interests separate from the communicated message and is driven by the desire to profit from a datafication of social relationships. The conclusion some theorists have drawn is that this process represents an intrusion into the privacy of our social relations and that enforcing privacy is a legitimate response to surveillance from government or corporate agencies.

Concerns are raised by media theorists about the methods of technologically mediated communications as well as the resultant behavioural changes. These changes may be influenced by an awareness of an undisclosed third party that has access to our social interactions or simply that they are stored somewhere. The IoT participates in this by accessing the same technologies but does so without notifying or interacting with the user. If an uninvited and concealed communication has taken place then any objections or concerns on the part of the user are rendered impossible. The IoT represents an intrusion of the internet into our physical space, preventing the possibility of choice. As a machine that is "fast, clever and relentless"[52], it requires neither our participation nor our consent. Indeed, its functioning depends largely on our ignorance.

Having considered the analyses of social media we can begin to place the IoT within this context. If we accept that technologically mediated communications can moderate or alter our behaviours then what happens in an environment filled with IoT devices, secretly communicating with our mobile phones? We might also assume that there is an apparent willingness on the part of users to allow their personal information to be publicly accessible and owned by corporate entities. At the very least, this transaction is made obvious from the moment of interaction with such a web service, as

52 "We are all data now," Vimeo video, 29:45, from documentary series Secret Society broadcast on BBC in 1987, posted by "Duncan Campbell," accessed 28 Sept. 2016. https://vimeo.com/49487288.

well as any time the user accesses it. Within the IoT there is no moment of transparency that demonstrates that such an action is taking place. We only have the possibility of always, everywhere and everything.

To begin investigating these questions this research will create a use-case scenario that uses off-the-shelf components and software written specifically to allow open examination of how the software functions. The scenario will be filmed in order to record the various parts inter-operating in a relatively explicit manner but will also retain the implicit elements hidden from casual observance. Inaudible audio signals transmitted can be considered as a bridge between the IoT light bulb and smart phone. The central role this plays is maintained in its purest form of the near ultra-high frequencies occurring at 18 kHz and above, albeit slightly amplified. This use-case is consistent with the ideas that underpin Critical Engineering by exposing the hidden aspects of technology.

CRITICAL ENGINEERING

/**/

// Methodology

To investigate the phenomenon of inaudible audio communication between IoT and smart phone, Critical Engineering provides a suitable methodology for examining technology and its implementation. The Critical Engineering Manifesto provides the methodological and philosophical basis of this project. The following key points declared in the manifesto are of particular interest:

- "study and expose"
- “observe... the space between production and consumption"
- "expose moments of imbalance and deception"[53]

These basic tenets are at the heart of Critical Engineering: practitioners are asked to examine the nature of a technology, how it has been constructed and, within that context, why it was made and how it might be used. By comparing the what and the how we may uncover side-effects that would otherwise remain hidden. If side-effects are produced, what ramifications might they have on the people who use this technology? Or are they not even side-effects but primary?

Central to this methodology is the idea that, as a form of critical enquiry, a technology should be examined "by means of digital excavation"[54] to extract its hidden components. These could be deliberately hidden by design or be present merely as a by-product of the complexity of contemporary technology, especially a computer-based one. Determining the logic behind a technological implementation can be as illuminating as the way it is used, as the boundaries of that logic can determine precisely what the technology is capable of. Critical Engineering, therefore,

53 “The Critical Engineering Manifesto,” Julian Oliver et al., published 2011, https://criticalengineering.org.
54 Ibid.

posits that uncovering the material construction of an object allows us to understand its components as having implications from the moment of construction. It is only within this context that we can determine whether or not a technology is functioning as we expect.

This method of research is aimed at observing a technology, seeking an accurate explanation and understanding of that technology and ultimately promoting a critical discussion about its implications. By making a Critical Engineering project, through the publishing of open source code, and other supporting materials developed for this project, it is hoped that the technology and processes investigated are sufficiently revealed to allow public examination. It is only with a full and open awareness of a technology that we can understand its use and meaning in our lives. It can also provide us with the ability to see aspects hidden from the lay observer as well as any unintended consequences that may arise from a particular implementation.

An illustration of the Critical Engineering methodology at work can be found in Julian Oliver's Transparency Grenade[55] which is an artistic intervention using technology to expose an audience to the ordinarily hidden wireless network traffic that exists all around us. The data gleaned using this device is sent to a server that extracts information such as images, websites, user-names and IP addresses. It is then presented back to the audience where the Transparency Grenade device is located. By doing so, this work asks the audience to consider that any action taking place on the internet is open to possible scrutiny by anyone or any other device.

Examining what an IoT interaction with a smart phone consists of will reveal both the method of its construction as well as its capabilities. With the use of Critical Engineering, my research will uncover that an integral part of the IoT landscape is the addition of secondary and hidden functions that are not obvious from simple observation. The research will utilise an off-the-shelf IoT light

55 "The Transparency Grenade," Julian Oliver, published 2012, http://transparencygrenade.com/.

bulb that appears to function as expected. However, within this item resides the secondary IoT component that provides all the means for it to become a new object and one that operates at a level beyond the mere observational.

Using the ideas of Critical Engineering this research will expose these functions hidden at the moment of manufacture by presenting them in the foreground. However, the hardware will still retain its obscurity as a close examination of the integrated circuit boards will not reveal anything other than complex circuitry. Instead, exposure will rely on foregrounding the effects of the IoT hardware and what it is capable of doing. Likewise a similar process of revealing is also used for the software components where functions commonly coded in the background of publicly available apps are examined for their effects.

// Project Introduction

Image: visual representation of an IoT light bulb communicating to a Smart Phone

The examination of the phenomenon of near ultra-high frequency audio transmission and receipt involves creating a Critical Engineering project that allows the examination of the components required. To begin, the marketing materials from industry press[56] and several of the main vendors (SilverPush, Signal360, etc.) were examined to develop a set of functional requirements. At a simplified level this involves utilising an IoT device on-board speaker system for transmission of audio and a typical smart phone for its receipt and processing.

// IoT Light Bulb

One of the key aspects of the IoT is that any object can be augmented with an IoT capability embedded inside it. To demonstrate this an IoT light bulb was chosen as it retains its appearance of

56 "Audio vs. beacons: Which is better at driving in-store engagements?," Chantal Tode, Napean LLC, Published 16 Dec. 2014, http://www.mobilemarketer.com/cms/news/messaging/19367.html.

being just that: a light bulb. By simply connecting a power source to the light bulb it will emit light, demonstrating that this is indeed a light bulb. For this Critical Engineering project the IoT light bulb is considered to function in a manner typical of other IoT devices. As such it can extend the infrastructure of the internet, is a semi-autonomous device and is an endpoint for data generation[57]. This is a particularly useful example of a new paradigm in which an object is no longer simply the object as defined by its appearance and typically defined purpose.

It is interesting that the advance in lighting has meant that light emitting diodes (LED) are used instead of a wire filament found in incandescent lights. There is a commensurate reduction in the physical space required for the LEDs that can emit a comparable amount of light, which in turn allows this redundant space to be filled with other things. In the case of this IoT light bulb, it is a pair of speakers, power distribution circuits and the circuit board containing the Bluetooth radio and audio processing capabilities. All of this is housed in an object that is of a similar size, shape and appearance to an incandescent light bulb.

The IoT light bulb chosen for this project has two audio speakers inside as well as a Bluetooth radio. The more expensive and advanced version by the same manufacturer has a Wi-Fi radio to enable a direct internet connection via the user's home network. Both types of light bulbs require the installation of a smart phone application to function beyond the simple power on-off normally associated with a light bulb. These secondary functions, such as colour, fading controls, as well as the Bluetooth connection, allow the light bulb to have audio transmitted to it for playback through its built-in speakers.

57 Australian Communications and Media Authority. *The Internet of Things and ACMA's areas of focus*. (Canberra: Australian Communications and Media Authority, 2015), 14.

The presentation of this IoT light bulb within this Critical Engineering project will reveal the light bulb's capacity for observation and analysis. Exposing these abilities in their rawest form allows the observer to reconsider an object that appears to function beyond expectation and in less obvious ways. These other functions are the heart of the IoT which embeds within everyday objects an internet connected computer to either augment the object's primary function or to add unrelated ones. The result of this process adds a level of ambiguity to any object that falls under the gaze of the IoT industry whereby the object that appears to be one thing is in fact another altogether.

Retention of the internet connection for this IoT light bulb is represented in the project by connecting it to a laptop that is itself connected to the internet and has a web page loaded that provides the audio signal source. This allows the extraction and extension of the typically hidden internet connection of an IoT device into the more recognisable domain of computer and web browser.

// Smart Phone Basic

The smart phone used in this Critical Engineering project is Android OS based, due to its low level development requirements and this researcher's familiarity with prototyping and developing custom applications. At a basic level the OS provides access to the device hardware as well as the software functions necessary to perform routine tasks. The Android OS also exposes several interesting API properties such as "android.media.property.SUPPORT_MIC_NEAR_ULTRASOUND" which is defined in the API documents as being: "Used as a key for getProperty(String) to determine if the default microphone audio source supports near-ultrasound frequencies (range of 18-21 kHz)". The same API level supports a similar property for the speaker of the smart phone.

There is not a requirement for speculation here as it is only important, following the methodology of this research, to reveal the existence of such capabilities at the point of design. The Android OS, therefore, has provided the means for a third-party developer to determine whether the phone their software is installed on can provide this particular near-ultrasound function.

From the built-in capability of the smart phone device hardware and software, the next stage is to consider examples of implementation. One type of mobile phone app researched came via a forked GitHub repository[58], which reveals that the code required for listening, recording and decoding any audio signal is usually packaged as part of a Software Development Kit (SDK). An SDK library is one that other developers could choose to include as a secondary part of their app. For instance the user of App A assumes that they have installed an app that provides some sort of game for them to play. The developers of App A have included third-party libraries that they deem a necessary part of their application and have done so without informing the user of this inclusion. These extra libraries could, for example, consist of adding the ability to send debug reports to a central server, displaying an advert overlay at specific times or enabling marketing analytics. This research is concerned with any library that is recording with the phone's microphone any near ultra-high audio that may be present and that can be decoded to reveal meaning.

Furthering the concept of the SDK library is one that is self contained, self reliant and does not depend on the running of the host application in order to function. This type of SDK library does so by running several background processes to fulfil the needs of its tasks while persisting in the background and waiting for certain conditions to be met. One of these conditions might be a sensor indicating the phone is on, is awake and is being used. Another might be to spawn a further process to periodically record the audio from the built-in microphone and listen for specific key conditions.

58 “SilverPushUnmasked,” MAVProxyUser, GitHub Inc, published 25 Nov. 2015, https://github.com/kaputnikGo/SilverPushUnmasked.

Unintentionally or otherwise, the addition of an SDK within a parent app does not have to be explicitly declared to the user of that app. In the example researched the only direct indication is derived from a specific permission declaration published on the app store. The declaration uses a broad "android.permission-group.MICROPHONE" that does not indicate how, when and why this permission is being requested. A library included in an app in such a way could be considered the equivalent of a trojan-horse that “masquerades as a useful service but exploits rights of the program’s user … in a way the user does not intend”[59].

59 Carl E. Landwehr et al, “A Taxonomy of Computer Program Security Flaws, with Examples”, *ACM Computing Surveys* 26, 3 (1994): 216.

IMPLEMENTATION

/***/

// Software Requirements

Similar to the way in which some voice activated applications function, this application listens for a particular preamble condition that indicates to the application that a qualifying message may be following. On popular mobile OS's this may be performed by the user saying a keyword, such as the name of the application and which is then followed by the message. In the case of our research application the preamble is a frequency (18 kHz) representing the letter A, which is then followed by a message consisting of other letters broadcast in alphabetical order. This simplified condition, of allowing letters increasing in alphabetical order, is to demonstrate a very basic method of minimising false positives that may occur when any audio is found that coincidentally matches our key frequencies. This is by no means a rigorous or production level standard, but is merely demonstrative of a required process.

The phenomenon investigated is of a sound wave that is audible to the phone at a particular frequency (18 kHz and above) and a particular decibel level. This sound wave could be intentional and a signal for this app to then continue listening for any more that may be recorded and check for any transmitted intelligence. To do so it can check these candidate sound waves against a list of alphabet characters that are each represented by a particular high frequency pitch above 18 kHz and separated by 75 hertz. Using such a method allows the space for the entire alphabet to be transmitted within the narrow range of frequencies that are considered beyond typical human hearing yet still recordable by a typical smart phone microphone.

// Software Description

For the purposes of this Critical Engineering project a custom app, named CFP_Ultra[60], is developed that utilises several Java classes to emulate several classes of functions typical of an SDK library. One of these classes retains its background process capability, so that there is an aspect of this app that performs its tasks in a way that is neither directly detectable nor accessible to the user. By placing the audio recording task in the background we can assume that the software component that facilitates a communication between the IoT light bulb and the smart phone is also hidden. By design the user is unaware and powerless to control the ability of this phone to listen for audio.

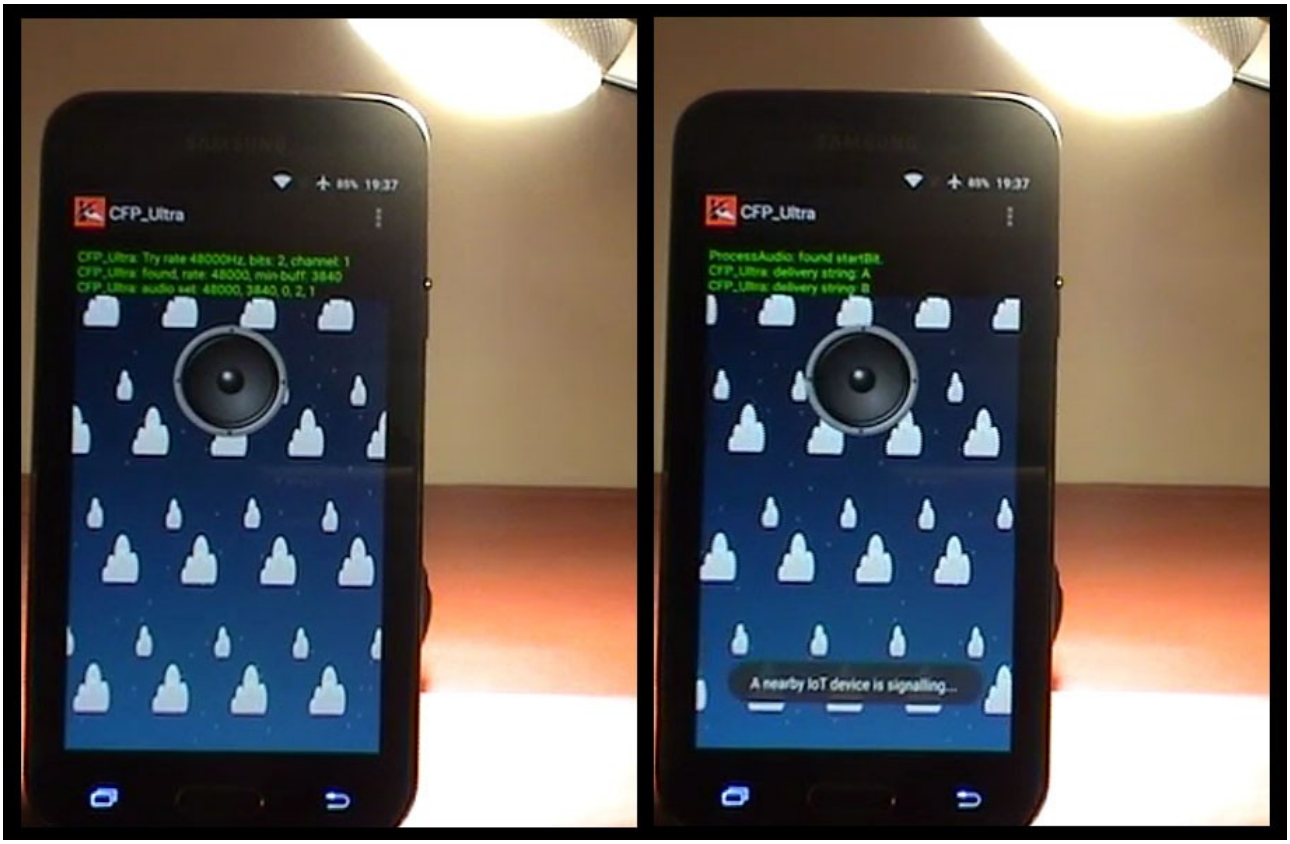


Image: screenshot from film of app initial state (left) and successful receipt of audio signal and toast display (right).

The purpose of CFP_Ultra is to present an interface that does, to a limited degree by design, inform the user as to what is occurring at runtime. The presentation of information consists of the major

60 "Android near ultra-high frequency listener," kaputnikGo, GitHub Inc, published 18 Aug. 2016, https://github.com/kaputnikGo/CFP_Ultra.

part of the app screen being taken up by a graphic of some clouds with a speaker cone in the foreground. At runtime these clouds are seen moving to the right and the speaker cone falls to the bottom of the screen with a bouncing motion that repeats for the duration of the app running. Partly meaningless and partly an abstract and satirical indication of what is occurring, the internet clouds are sending audio directly to the microphone typically located at the bottom of the device.

At the top of this graphical scene is a representation of a console log output which consists of several lines of green text on a black background. The console log is a function used by apps for debugging, allowing a given app to write lines of text to a file located in the phone's operating system. Typically this can range from statements of the occurrence of important events to the cause of the application's failure or crash. In the CFP_Ultra app several key statements are made to describe its current state using a terminology that is perhaps meaningless to the casual observer but useful to the developer for debugging.

When the app is running this console log output displays several statements that appear to be linked to an event but give no indication of what that event is. Several of the words included in these statements may prompt some thought or concern in this context: "Detector", "record" and "ProcessAudio". Following these are a stream of messages that have a letter at the end that increases alphabetically. If these are not noticed, the app utilises a form of notification system that is intended to be seen.

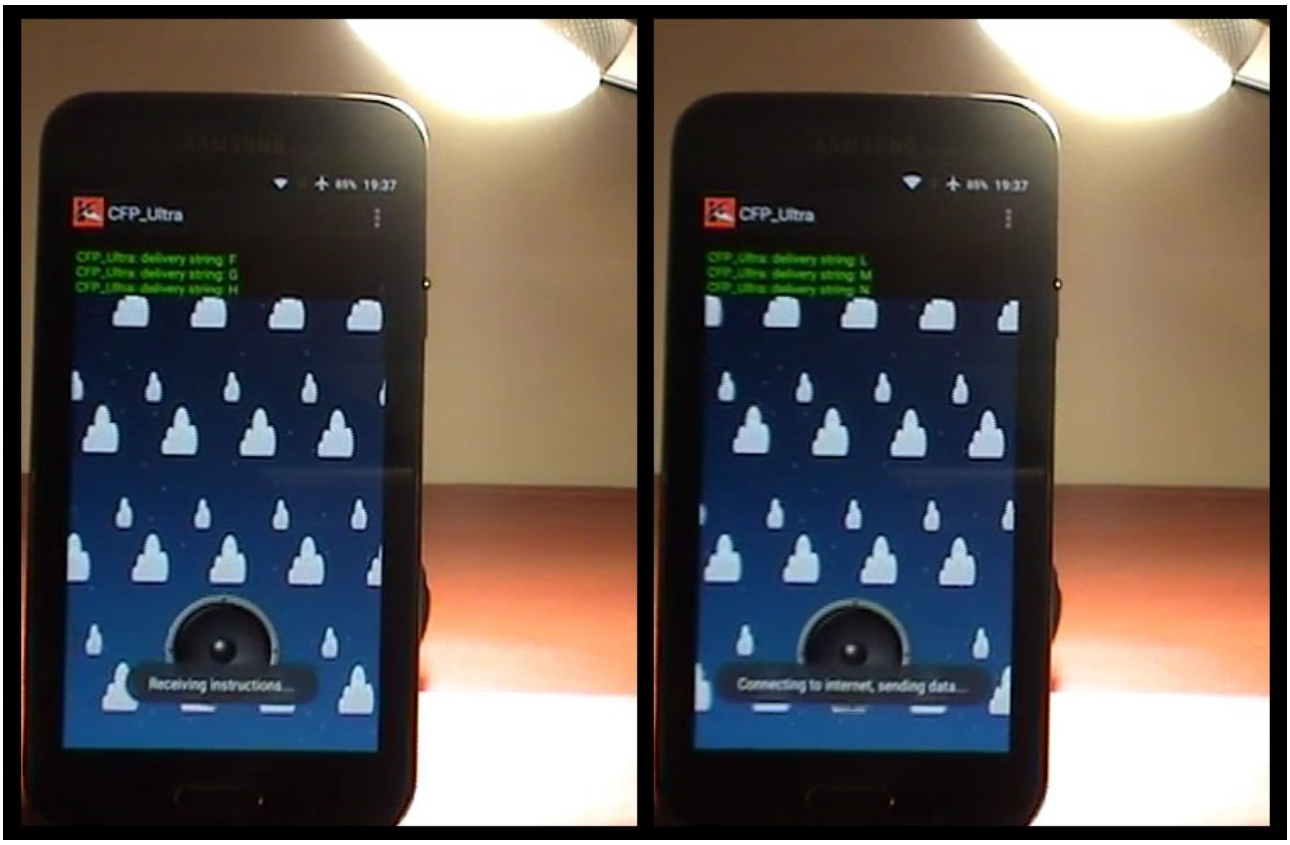


Image: screenshot from film showing toast messages displayed based upon intelligence received from IoT light bulb.

The use of system provided notifications (toasts) is chosen as it can offer a one-way broadcast message that has no scope for user interaction. As such it can serve to further highlight the disconnect between the user and the technology they use. The statements contain phrases that provide limited meaning for the average user: “nearby IoT”, “device is signalling”, “receiving instructions”, connecting to internet, sending data”. These messages are so generic that any meaning would only be possible when a full and proper understanding of their context is made.

Consistent with the Critical Engineering method of bringing hidden processes to the foreground, these toasts announce in a generalised and limited way that something is occurring with the device that was instigated by a nearby IoT device. The intention here is to present both the ambiguity and uncertainty for the user as to what, precisely, is occurring. The provision of these toast messages also serves a secondary purpose: to inform the user that they no longer have the ability for input, for

consent or for refusal. A quick thinking user may choose to either switch the phone to aeroplane mode or even turn it off. Even assuming this rather extreme action on the part of the user they are left with a semi-functioning mobile device and uncertainty as to when to revert the device to its normal operating state.

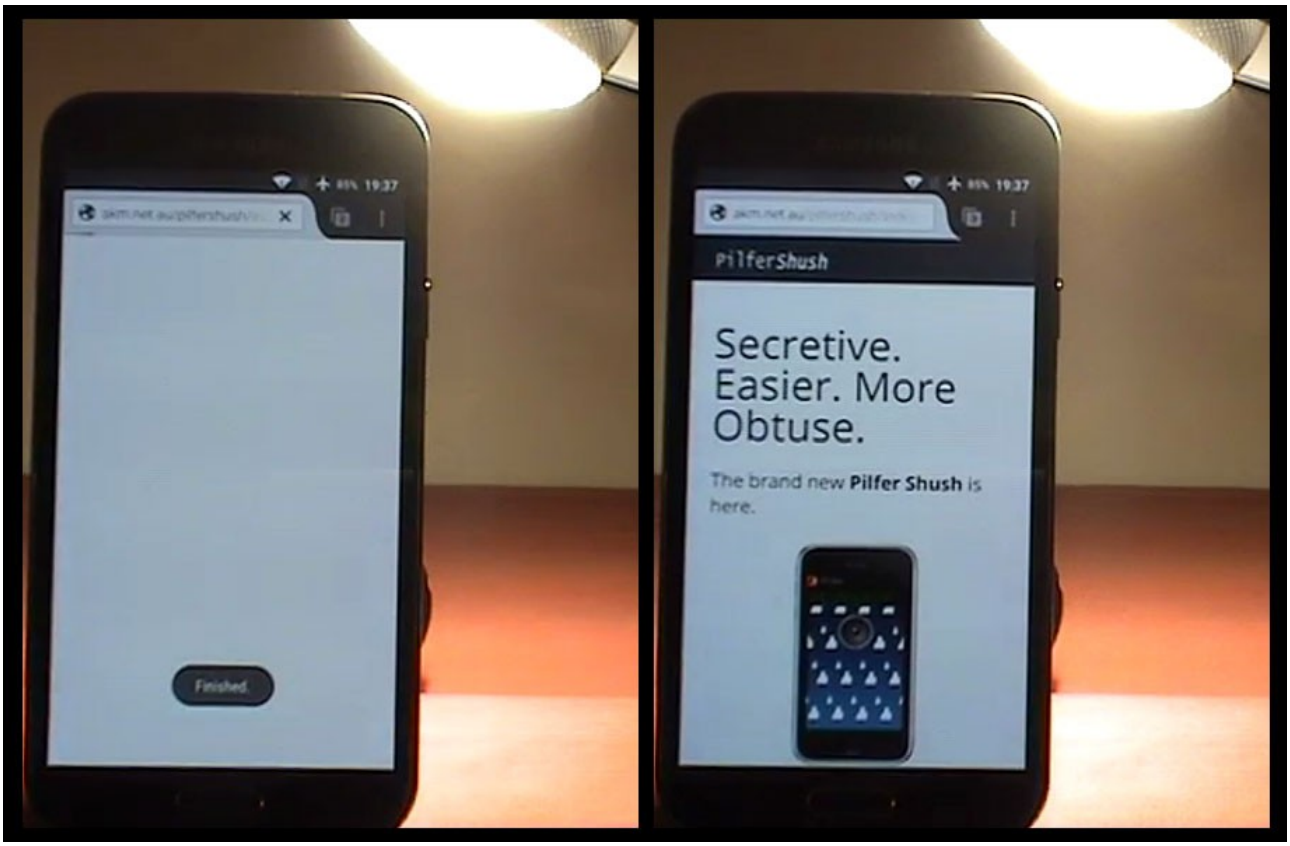


Image: screenshot from film showing end of signals and spawning of web browser

After the appearance of several of these toast messages the phone then automatically opens the system default web browser, connects to the internet and loads a website landing page for this project[61]. The process used here is one that seeks to make known and visible the otherwise hidden internet connection that occurs when an IoT device communicates with the phone. A web page is a tangible and known result of an internet connection but is only one of many. Many apps will communicate with their vendor servers for the purpose of exchanging data not meant for rendering

61 "PilferShush," s3204584, accessed 30 Sept. 2016, http://akm.net.au/pilfershush/index.html.

in a browser. An example would be an app updating in the background the user's location data in longitude and latitude so that a search query for "best pizza in town" will return localised results.

A lack of comprehension is one way that the user of a smart phone can succumb to a sense of powerlessness. The complexity of technology in general often renders its function incomprehensible to the lay user. But even if we cannot describe how a television works, its use is apparent when we see the moving images on the screen and hear the sounds from its speakers. The lack of comprehension about how we are able to use this technology is offset by our understanding of why we use it when we watch our favourite television programme. So too for the smart phone, that seems to be able to inform the user that the best pizza place is right around the corner.

Powerlessness produced by the failure to understand how something happens could be extended to include a powerlessness to understand why something happens. With only a basic understanding of how our smart phones function it is not possible to comprehend the complexity of these small nondescript rectangles we carry with us everywhere we go. Indeed, these smart phones tend to operate independently of the user and direct control is only possible when the user selects a user interface item such as a button. After that moment of interaction there is little control available as the device commences executing software functions invoked by that simple touch.

The use and purpose we give a technology provides a tangible interface that connects us to the mystery of its technical complexity. While this idea may not be articulated every time we access a website or traverse the internet, it can function as a kind of power relationship. In this relationship the user can be made aware that what they are doing is derived from the responses of the interface to this complex machine. The web page shown on the computer screen sufficiently informs us of what we may need or care to know about how it came to be displayed. Herein lies a power

imbalance where the user has to accept in good faith that the effects presented by the technology, the web page, is an accurate portrayal of what was requested.

When we are in an environment containing IoT devices secretly communicating with our smart phones that in turn are undetectably connecting to the internet, our awareness is diminished. A conceptual barrier is placed between us and the technology that we use. There is no effect or response we can extrapolate from an interface to indicate that an interaction has occurred. There is also no indication of the type of interaction, nor of its intentions or motivations.

// Software Development

Conducting research following the Critical Engineering methods resulted in the CFP_Ultra software application being developed. It serves the role of the parent app that houses the hidden audio recording functions, known as PilferShush. It has been published on GitHub[62] in order to allow the functions to be examined via the source code. The application code layout consists of a main activity class that serves as the user interface, a background service class to periodically access and poll the hardware microphone, a recording class, frequency analyser class, decoding audio value class and an implementation of the Goertzel algorithm[63] to determine candidate frequencies.

Each major component of the application has its own class with all the associated functions that it may need to properly perform its tasks. These chosen classes allow the application to meet the requirements of listening to any audio via the on-board microphone, periodically performing a check to determine if a particular frequency is heard and then listening for any subsequent audio that matches certain criteria. It does this in a manner that allows some visual cues to the user of the

62 “Android near ultra-high frequency listener,” kaputnikGo, GitHub Inc, published 18 Aug. 2016, https://github.com/kaputnikGo/CFP_Ultra.

63 Kevin Banks, “The Goertzel Algorithm.” *Embedded Systems Programming* 15, 9 (2002): 34.

smart phone as to what is occurring at any time, but mainly is intended to be a piece of open sourced demonstration code.

The class tree and description based upon the UML (see Appendix A) is presented below:

- com.cityfreqs.cfp_ultra
  - MainActivity.java
  - UltraService.java
- com.cityfreqs.cfp_ultra.pilfershush
  - FreqDetector_Goertzel.java
  - Goertzel.java
  - ProcessAudioValue.java
  - RecordTask.java

MainActivity.java : The Activity is an application component that provides a screen with which users can interact in order to do something, such as dial the phone, take a photo, send an email, or view a map (https://developer.android.com/guide/components/activities.html). This class provides the only interface screen that the user will see when using the CFP_Ultra app.

UltraService.java : A Service is an application component that can perform long-running operations in the background and does not provide a user interface. Another application component can start a service and it will continue to run in the background even if the user switches to another application. For example, a service might handle network transactions, play music, perform file I/O, or interact with a content provider (https://developer.android.com/guide/components/services.html)

This class runs in the background, calls the audio recording classes, listens for any signals that may be received and informs the main activity if found.

FreqDetector_Goertzel.java is the class that makes requests for background recording of audio captured by the host device hardware microphone. It does so by periodically calling the RecordTask.java class which handles the actual recording methods. It checks whether there are candidate signals that consist of the required frequency range and amplitude.

Goertzel.java is an implementation of an algorithm[64] intended to determine if candidate frequencies are present in an audio signal.

ProcessAudioValue.java is the class that performs a comparison of frequencies that match against a list of alphabetical characters. It also performs various checks on the characters received and informs the MainActivity class of any sequence of letters.

RecordTask.java performs the listening functions and runs the first checks on any audio that may become a candidate signal. This check ensures that any potential audio intelligence occurs above a determined minimum frequency and magnitude. It relies on the Goertzel algorithm for this task.

When a candidate message sequence is received CFP_Ultra's service sends each character to the main activity which then checks if that letter matches a pre-set condition. If these conditions are met then, depending on the case, the application calls another function that represents the instructions received from the IoT light bulb. In our case these instructions merely invoke system toast messages that display some non-actionable information to the user and ultimately cause the phone’s web browser to connect to the internet and display a web page.

64 Kevin Banks, “The Goertzel Algorithm.” *Embedded Systems Programming* 15, 9 (2002): 34.

// Demonstration

Image: Use-case scenario scene

The demonstration of inaudible audio communicating with a smart phone poses several challenges if the intention is to directly convey meaning. The demonstration a phenomena occurring undetectably in one medium could be transferred to another that is more identifiable such as graphical imagery. It could also take advantage of some form of analogy such as transcribing a digital concept into a paper analogue[65]. The risk here is that parody or analogy would ultimately fail to communicate the simple yet unique circumstance of its existence. A translation or an over-simplification is not necessary, the phenomenon of interest here is not particularly complex once it is broken down into its fundamental parts.

To demonstrate the inherent ambiguity of the use-case scenario the research project has been filmed to show a short demonstration of the IoT light bulb communicating with a smart phone running the

65 "Attorney-General George Brandis struggles to explain Government's metadata proposal," Sarah Dingle, ABC Online Services, 7 Aug 2014, http://www.abc.net.au/news/2014-08-07/brandis-explanation-adds-confusion-to-metadata-proposal/5654186.

open source CFP_Ultra app. The contrived scenario sees the IoT light bulb audio-in line connected to a laptop which in turn is connected to the internet. The laptop browser visits a web page consisting of HTML 5 and JavaScript code (also available with the app source code) that enables a synthesiser to play specific audio tones in the near ultra-high frequency ranges of 18 kHz to 20 kHz. These audio tones are listened for by the CFP_Ultra app that is running on a smart phone located within range of the transmitting IoT light bulb.

As the image above, and the film shows, there are several components visible, from left to right, that need describing. The first is the phone, mounted on a shop display stand, that is running the CFP_Ultra app. The display stand was chosen as it symbolises the singular and ultimate choice the user has in the purchase of a smart phone. Displayed, on its altar, the phone beckons with the power and mystery of a complex technology contained within a consumer desire.

The desk lamp housing the light bulb is a cheap, off-the-shelf lamp purchased from a High Street shop. It is mass produced and available with no variations in colour or size from a multitude of chain stores across the country. The light bulb inside pokes out only enough to allow an assessment of whether there is a light bulb present. Its very nature, its IoT abilities, are hidden not just within the light bulb but also the lamp shade itself.

The positioning of these two components is a deliberate display of the relationship between these two objects in this scenario. The lamp is positioned looking down upon the phone in the pose of an interrogator’s light. Its focus is clearly directed at the phone which is angled up towards the light. It is a visual hint at an imposed power imbalance where the smart phone is subservient to the IoT light bulb and its transmissions.

Next are two circuit boards made for this demonstration. The brown board is a simple circuit with one bus to distribute power from the power supply to the desk lamp cable. The second bus takes the audio from the amplifier and also connects it to the desk lamp cable. The green circuit board is a shop bought kit that amplifies an audio signal. This circuit is included as the audio derived from the laptop headphone socket was too quiet for the IoT light bulb speakers.

Both the IoT light bulb lights and the audio amplifier required power, which was delivered by a regulated power supply that converted 240 volts mains electricity into 6 volts DC. The level at which the amplifier amplifies the audio is in direct relation to the amount of current supplied to it and, after experimenting, 6 volts was determined to be nominal.

Finally there is a laptop displaying a browser application that has loaded the web page specifically coded for this research project. The page uses HTML 5 and JavaScript to generate tones of audio at specific frequencies, much like an electronic synthesizer would. These tones are then sent via the connected headphone cable to the amplifier mentioned above.

During the demonstration in the film several graphical elements are seen to be appearing or changing as the demonstration progresses. The meanings behind these elements are as opaque to the viewer as the language of computer programming is to the lay user. Some of these graphical elements, for example the toasts, may be recognisable to users of smart phones running the Android OS but what prompted their appearance, what constitutes their meaning, remains a mystery. However, there is one clearer moment in the demonstration video that occurs when a browser window suddenly appears with a page loaded in it. The loading of this page occurred without the direct command of the user, but rather appeared as if of its own accord.

The loading of this web page is a direct indication of a connection to the internet being made. It is also the indication of the loading of a specific web page. While I have avoided analogies in general, this case lends itself to analogy. An internet connection and the transferring of data does not need to take place with a browser. Data connections can and do take place within many apps for a multitude of reasons and to exchange a multitude of different types of data. For my research to remain consistent with the Critical Engineering methodology, it is important to foreground any hidden processes involved in the phenomenon I am investigating. The transference of data via an internet connection is another aspect that is also hidden from the user when it takes place entirely within the app. By showing the phenomena directly in such a manner we are able to imagine what this might mean to a user, unencumbered by a specific vendor implementation.

// Examination

What might this demonstration mean to the observer? Demonstrating an inaudible audio communication between an IoT light bulb and smart phone allows only a simple conclusion to be made at this point: an IoT device is capable of communicating with our smart phone without our knowledge, input, understanding or consent. In order to understand why this is occurring and indeed why it might give rise to concerns, the Critical Engineering methodology that seeks to expose the inner workings is required. To reveal something is to presuppose it was hidden in the first place. However, several of the components of this technology might be understood to be hidden merely by their complex nature.

We must look into why a technology is hidden and what benefit could be derived from such an act. It is also necessary to acknowledge that this act of hiding renders the user powerless and does so without their knowledge. If the user of the smart phone did not want their personal information to

be gleaned from their device and transmitted to some unknown server somewhere on the internet they have little recourse: they have neither an awareness of this process nor an option to decline it.

Of course, if this technology is deployed by the advertising/retail industries then we may start receiving more personalised, time and location specific adverts on our devices. While this might be considered a benign use of the technology, this particular implementation does not concern us. Rather, it is the ability itself that is of concern: the communication that is directed at our phones, for reasons unknown, that we cannot control.

DISCUSSION

/**/

The main investigation for this research centres around the phenomenon of inaudible audio signals between an IoT device and a smart phone. Not only is the communication designed to be hidden from the user but it also causes their smart phone to connect to the internet and transmit data about the user to a third party web site. The problem of a communication between an IoT device and smart phone is made more pronounced when it is considered within the context of real world deployment.

By following the methodology of Critical Engineering the various components necessary for an IoT to smart phone communication were digitally excavated for analysis. From these hardware and software elements a use-case scenario was developed with the intention of foregrounding the hidden elements via the production of open source code. To aid this a video was made that recorded the demonstration an IoT light bulb interacting in some way with a smart phone. It allowed me to examine an IoT device communicating some form of intelligence to a mobile phone in a manner that is not discernible by typical human sensory capabilities. The film demonstrates that we are still left with ambiguities and uncertainties if not a complete ignorance that anything is in fact occurring.

From first examination the film shows a light bulb in a lamp, next to which is a mobile phone. The phone runs an application that reveals neither its origins nor its purpose. Several actions are seen to take place that also don’t appear to relate to anything tangible until the end when a web browser window opens and a product landing page is displayed. In this example the product web page is for the IoT light bulb itself but this type of connection made to the internet can be for any number of

purposes. It can also be made entirely within the background of the app and never reveal any of its communications to the user.

As IoT devices are propagated through the physical environment we are left to consider what course of action might be possible for those wishing to avoid this type of communication. Is our ability to contest their use possible if we wish to retain an ability to participate in social life? Answering these questions requires consideration of the different contexts technology can produce and how they may force us to rethink established social and legal norms around privacy. There is a fundamental contradiction at the heart of contemporary privacy debates: that consumers often tacitly, if not explicitly, consent to privacy incursions, thus undermining the very concept of privacy itself.

The arrival of the IoT environment means that we can no longer simply avoid privacy invading technologies, they surround us. The contexts of their implementations are multiple and the subsequent responses from society are varied. A precedent for this has been made visible in social media networks (i.e. Facebook, Instagram, Twitter, etc.) where the users of a given platform willingly provide content from their private lives for public display. This active participation reveals a significant shift: what may have once been considered to be the sanctity of the private realm is now a public commodity. These platforms, however, still allow us to be aware of this and offer some forms of control via privacy settings.

While the role of Critical Engineering is useful in providing an experimental framework and methodology for this project to generate observational data, we also need to make sense of this data within the context of where and how it would normally be encountered and the possible rationale for its use. We also need to determine if the IoT technology discussed in this thesis is operating at a level that would cause us concern over privacy issues. To help formulate thinking around this the

legal profession offers a perspective on how technology should be allowed to interact with us and how it can infringe what may be considered to be rights, such as privacy or the right to be left alone. Lawyers and policy makers have invested considerable time and effort into establishing a functional vocabulary to use in the arguments for or against a technological implementation.

To develop a framework for understanding privacy issues we can focus on the analysis of academics, theorists, commentators and legal professionals primarily within the European Union and the United States. These two locales have their own idiosyncratic historical and cultural contexts that inform ideas and opinions around privacy, its definition and use. For example the EU may be influenced by its desire to amalgamate into a single, unified economic union from a "people of dissimilar backgrounds and cultural assumptions"[66]. The US on the other hand has a rich history of legislating and protecting privacy not only via constitutional law but also via key court cases such as Katz v. United States[67].

At the very forefront of this discussion on privacy is the need for the individual to be aware that an issue or a concern regarding privacy is being raised. It is also necessary that the person concerned has their own, perhaps latent, definition of privacy and private matters. As well as this there is need for an awareness of whether the technology being examined threatens in some way any of the elements that constitute the enactment of personal privacy. The idea that the concept itself is outdated further, compounds any debate on privacy.

Some of the loudest oppositional voices to any perceived privacy violations are the opinions of Eric Schmidt and Mark Zuckerberg. The business model of the two companies they represent rely on the ability to gather personally identifiable information on their users. Responses to privacy concerns,

66 Nick Bostrom and Anders Sandberg. *The Future of Identity.* Oxford: Oxford University, 2011: 49.
67 *Katz v. United States*. 389 U.S. 347 (1967).

such as "maybe you shouldn't be doing it in the first place"[68] and "privacy was no longer a social norm"[69], reflect the interests of those who stand to benefit from the progressive erosion of privacy. Given the popularity of the services offered by these two companies it must be acknowledged that the user may not be concerned about privacy in this context. A further consideration is that these same CEOs have also given expression to the idea that people are prepared to relinquish some of their privacy and that they show a "willingness to engage in their own exploitation"[70] for the chance of some beneficial return.

The context of technology involving computers, data collection and storage has been the impetus for several implementations of privacy laws. These laws, such as the Privacy Act of 1974[71], were direct responses to concerns raised by academics and the wider community. However, according to some research, privacy is increasingly infringed and eroded indirectly, and legal protection against these privacy violations cannot be codified effectively by current law. In order to investigate this, policy research has considered not just the "collection and usage practices" but also the "basic values that are challenged by the changes brought by a networked society"[72] in which the historical division between public and private may no longer be relevant.

Placing this within the IoT context we can still ask: does the IoT infringe legal rights and definitions of privacy? Does the extraction of personally identifying information (PII) by third parties invoke concerns for the individual about their own privacy? On the other hand, if we focus on the vendor, is it cause for concern that this IoT technology seeks to function the way it does, without the user's

68 "Google CEO On Privacy: If You Have Something You Don't Want Anyone To Know, Maybe You Shouldn't Be Doing It," The Huffington Post, Published 18 Mar. 2010. http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html.

69 "Privacy no longer a social norm, says Facebook founder," Bobbie Johnson, Guardian News and Media Limited, Published 11 Jan. 2010, https://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

70 Nancy K. Baym, "Social Media and the Struggle for Society." *Social Media+ Society* 1, 1 (2015): 2.

71 *Privacy Act of 1974*. 5 USC Sec. 552a. S. 3418 (1974).

72 Simone Fischer-Hübner et al. "Online Privacy: Towards Informational Self-Determination on the Internet." Dagstuhl Manifestos 1, 1 (2011): 6.

awareness, as well as accessing PII for reasons unknown and stored and distributed by parties unknown for time unknown?

// Issues and Questions

A need for a coherent definition of privacy necessarily arises in the "context not only of place, but of politics, convention, and cultural expectation"[73]. Each of these contexts can be either "sweepingly defined"[74] or "finely drawn"[75] and this broad range may influence how privacy is understood. Helen Nissenbaum also suggests that a jurisprudential analysis of the historical context in which the "public and private define a dichotomy"[76] has "proven useful in legal and political inquiry"[77]. However, an observation of human behaviour has demonstrated that we are "not only crossing dichotomies, but moving about, into, and out of a plurality of distinct realms"[78]. To determine a theory of privacy therefore requires an acknowledgement that the dynamic ways in which people interact may not suit neatly definable categories.

If we cannot simply refer to a clear and definable private sphere to provide a definition then it may prove useful to consider privacy from the perspective of the individual and the context in which they feel that it has been violated. Nissenbaum uses data mining and Radio Frequency Identification (RFID) tags, as examples of "public surveillance"[79]. So far, developing a legal response to this has been hampered as "traditional theoretical insights fail to clarify the sources of their controversial nature"[80]. Even without tangible policy being enacted, most research into this area suggests that there is a need to "articulate a justificatory framework for addressing the problem of public

73 Helen Nissenbaum, “Privacy as Contextual Integrity.” *Washington Law Review* 79 (2004): 137.
74 Ibid.
75 Ibid.
76 Ibid.
77 Ibid.
78 Ibid.
79 Ibid., 119.
80 Ibid.

surveillance"[81]. Despite the failure to legally determine if surveillance occurs in this manner, the effects of a public assuming it takes place needs to be addressed.

Research into the impact of privacy incursions via surveillance, especially post-Snowden documents, has demonstrated that surveillance "significantly chills one's willingness to publicly disclose"[82]. This withdrawal has the potential to "pose a threat to democratic discourse" especially if an individual feels that they have "unpopular political beliefs"[83]. Elizabeth Stoycheff analyses a recent internet based survey, in which only "57%" of respondents believed surveillance in this manner to be unacceptable. Notwithstanding the 43% who reported being unconcerned, surveillance, according to Stoycheff, remains important in "influencing conformist behaviour"[84]. The idea that "public opinion is the opinion which can be voiced in public without fear of sanctions"[85] may seem far removed from an environment containing IoT sensors. However, technology can enable surveillance and it is the intention of this thesis to investigate whether the IoT is performing such a role by generating data that is used by either government or corporate actors to identify people and their characteristics. At the centre of this is the notion that there is an inherent conflict between the individual desiring privacy and the larger entities attempting to succeed in infringing upon it.

Concerns around privacy are not just exclusive to the individual: there is a growing awareness of privacy issues and the need for a regulatory response by industry itself. Given that IoT devices "increasingly detect and share observations about us", industry is becoming eager to respond to the

81 Ibid., 123.
82 Elizabeth Stoycheff, “Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring.” *Journalism & Mass Communication Quarterly* 14, 3 (2016): 1.
83 Ibid., 2.
84 Ibid.
85 Elisabeth Noelle-Neumann, “The Spiral of Silence a Theory of Public Opinion.” *Journal of Communication* 24, 2 (1974): 44.

community desire for "appropriate security and privacy protections"[86]. This response would have to balance the concerns of the individual and the commercial imperatives of a nascent industry. Commercial benefits are a consideration when the propagation of IoT devices are expected to provide for vast economic growth via the estimated "25 billion connected devices"[87]. Commercial considerations may also explain the latest response from the US Federal Trade Commission which announced that "legislation aimed specifically at the IoT at this stage would be premature"[88].

A further complication arises when policy makers seek to legislate based on a perceived need for privacy protections while normative behaviour in the wider community suggests otherwise. Consumers are complicit in privacy infringements when they use consumer-targeted technology that enables surveillance, tracking and observation. This “form of citizen engagement”[89] is referred to as “Participatory sensing”[90]. From the seemingly innocent baby monitor to the *quantifiedself.com* movement, we have actively sought out and engaged with technology that has enabled a "tolerance for watching and being watched, measuring and being measured"[91]. Our participation in this is something that can "reshape our relationships across multiple domains of daily life" and this can incur additional "complex implications for privacy"[92].

86 Federal Trade Commission. Internet of Things: Privacy & Security in a Connected World. (Washington: Federal Trade Commission, 2015), 55.
87 Ibid., 1.
88 Ibid., 49.
89 J. Höller ed., *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*. (Amsterdam: Elsevier Academic Press, 2014), 295.
90 Ibid.
91 Karen E.C. Levy, “Relational Big Data.” *Stanford Law Review Online* 66 (2013): 79.
92 Ibid., 74.

CONCLUSION

/**********/

Referring to other theories enables a deeper understanding of the problem by transplanting it into different disciplinary fields such as Nissenbaum's use of contextual integrity or a descriptive analogy such as economic sociology[93], or digital curtilage[94]. This theoretical expansion can occur because of the various new connections that can be made between elements germane to the problem and responses from the theory.

Within a domain as complex and sometimes convoluted as privacy, it is necessary to be aware of concerns that have previously been raised and attempts to contextualise them. It is also important to recognise that proposing laws to cover a new aspect of society is particularly fraught when differing perspectives are competing with one another. On the one hand some users willingly participate in an action that others would consider an invasion of privacy. On the other hand, some vendors have admitted that they push the private/public boundaries until they provoke a suitably powerful reaction against it. At the forefront of this problem is the IoT environment that operates at a level outside a communicable infringement on privacy and instead is based upon remaining hidden.

Does the act of hiding a technology, that some may consider privacy invasion in and of itself, give rise to concern? Attempts by researchers to frame this problem have been instructive in revealing its inherent complexities. This thesis' specific use-case scenario in the IoT environment has demonstrated that some of the participants remain unaware that the IoT is around them. Exacerbating this problem is the fact that a specific branch of the IoT industry is developing a technology intended to be invisible to the lay person and that this technology is designed to acquire

93 Ibid.

94 Andrew Guthrie Ferguson, "The Internet of Things and the Fourth Amendment of Effects." *California Law Review* 4, 101 (2016): 162.

and process personally identifiable information for the economic benefit of the vendor and do so automatically via the internet.

A typical smart phone user will have only limited awareness of whether their phone is connecting to the internet and exchanging data with websites and services. Some processes remain tangible, visible and controllable, such as a browser loading a web page or a push notification. In contrast is the IoT device that is hidden within another object or embedded within the environment ensuring the user remains ignorant of its existence.

It is the purpose of these devices in effect to secretly communicate with any smart phone within range in order to initiate a data connection to transmit information to a server somewhere. It is not the concern of this research to investigate the range of specific types of information that maybe transmitted. This research must equally allow for communicated information that is either benign or harmful, intentional or otherwise. With this consideration in mind it is then possible to assess the technology we have described at a more basic level to determine whether there are fundamental privacy concerns.

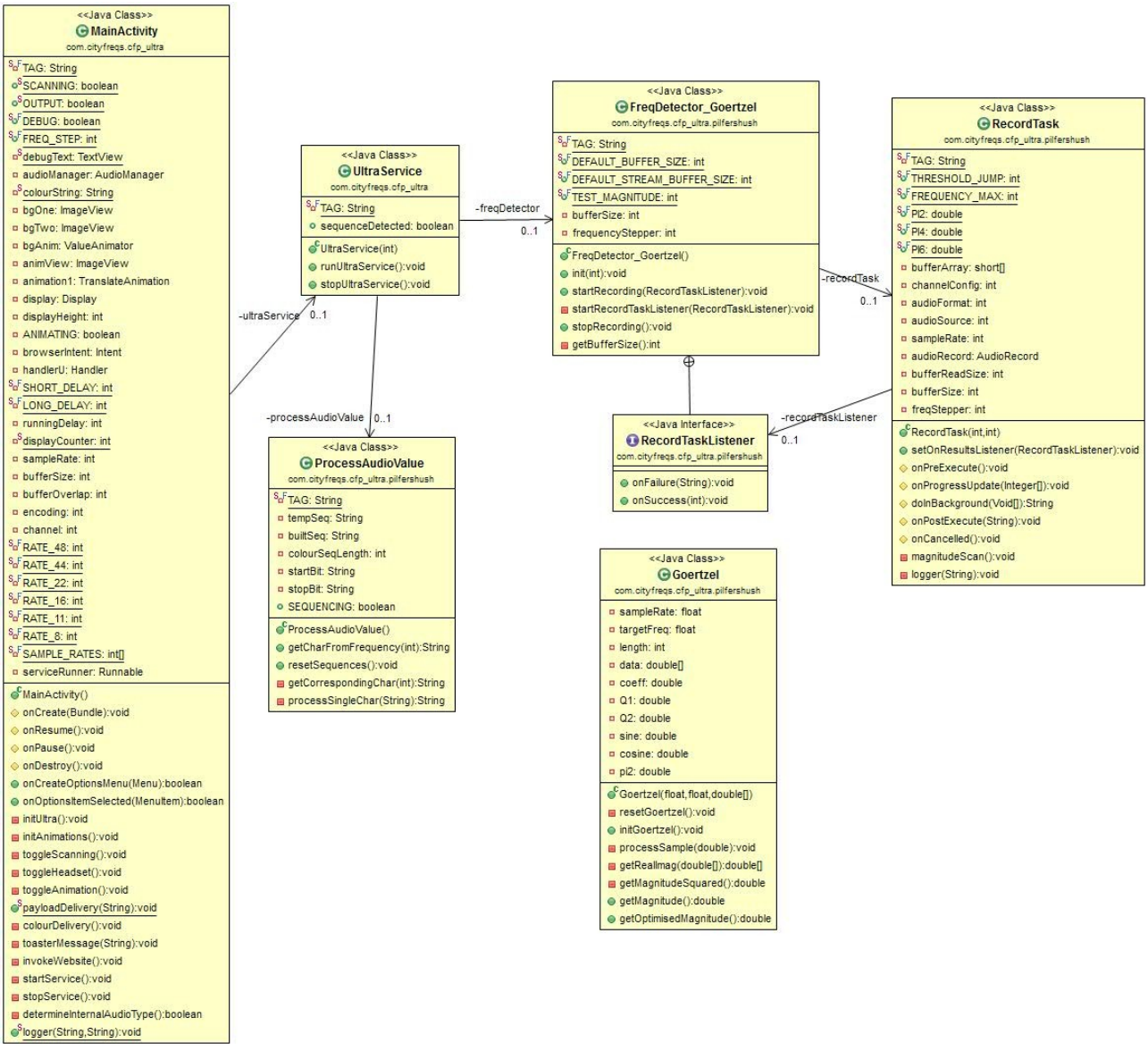
Should this type of hidden communication, in itself, be considered an insidious threat? It is possible that a vendor may not be seeking permission because they are concerned that permission will not be forthcoming. In contrast to the vendor perspectives are the normative behaviours associated with social media use, i.e. a majority of users seem to at least tacitly accept a lack of privacy and associated controls. Many users accept that the private corporate entities providing social media platforms can and do collect and trade for financial gain any of the user content uploaded to the servers. There seems to be an acceptance that there is a beneficial transaction of personal

information for consumer information. Even so, the user of such a technology still retains a degree of choice and an awareness of what that choice may entail.

My research, source code and filmed use-case scenario have demonstrated that the vendor providing the IoT audio beacon technology does so knowing that it is hard to detect and hard to determine its specific behaviours. We can assume that there are instances where an individual might not desire such an interaction or at the very least might expect to be offered a request for permission. The desire for knowledge about a communication technology is motivated by the desire to exercise control over it. This in turn describes how an individual is presented to the outside world and within what context. These concerns are the domain of the individual user and not to be confused or diluted by the IoT vendor’s intentions. The motivation for deploying this technology is irrelevant when its function is, at the moment of its conception, hidden from observation in a manner that can only be interpreted as deceptive and devious.

APPENDIX

****



Appendix A: UML diagram of CFP_Ultra app at time of last compile.

BIBLIOGRAPHY

Australian Communications and Media Authority. *The Internet of Things and ACMA's areas of focus.* Canberra: Australian Communications and Media Authority, 2015.

Banks, Kevin. "The Goertzel Algorithm." *Embedded Systems Programming* 15, 9 (2002): 34–42.

Baym, Nancy K. "A Call for Grounding in the Face of Blurred Boundaries." *Journal of Computer-Mediated Communication* 14, 3 (2009): 720–723.

Baym, Nancy K. "Social Media and the Struggle for Society." *Social Media+ Society* 1, 1 (2015): 1-2.

Bostrom, Nick, and Anders Sandberg. *The Future of Identity*. Oxford: Oxford University, 2011.

Dıaz-Moralesl, Roberto. "Cross-Device Tracking: Matching Devices and Cookies." *2015 IEEE International Conference on Data Mining Workshop* (2015). 1699-1704.

Elwell, J. S. "The Transmediated Self: Life between the Digital and the Analog." *Convergence: The International Journal of Research into New Media Technologies* 20, 2 (2014): 233–249.

Ferguson, Andrew Guthrie. “The Internet of Things and the Fourth Amendment of Effects.” *California Law Review* 4, 101 (2016): 101-176.

Fischer-Hübner, Simone, Chris Jay Hoofnagle, Ioannis Krontiris, Kai Rannenberg, and Michael Waidner. “Online Privacy: Towards Informational Self-Determination on the Internet.” *Dagstuhl Manifestos* 1, 1 (2011): 1–20.

Federal Trade Commission. *Internet of Things: Privacy & Security in a Connected World*. Washington: Federal Trade Commission, 2015.

Gaglio, Salvatore, and Giuseppe Lo Re, eds. *Advances onto the Internet of Things*. Advances in Intelligent Systems and Computing, Vol. 260. Cham: Springer International Publishing, 2014.

Höller, Jan, ed., *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*. Amsterdam: Elsevier Academic Press, 2014.

Katz v. United States. 389 U.S. 347 (1967).

Landwehr, Carl E., Alan R. Bull, John P. McDermott, and William S. Choi. “A Taxonomy of Computer Program Security Flaws, with Examples”, *ACM Computing Surveys* 26, 3 (1994): 211-254.

Levy, Karen EC. “Relational Big Data.” *Stanford Law Review Online* 66 (2013): 73-79.

Nissenbaum, Helen. “Privacy as Contextual Integrity.” *Washington Law Review* 79 (2004): 119-157.

Noelle-Neumann, Elisabeth. “The Spiral of Silence a Theory of Public Opinion.” *Journal of Communication* 24, 2 (1974): 43–51.

Privacy Act of 1974. 5 USC Sec. 552a. S. 3418 (1974).

Ratto, Matt. “Critical Making: Conceptual and Material Studies in Technology and Social Life.” *The Information Society* 27, 4 (2011): 252–260.

Smith, Steven W. “Audio Processing.” In *The Scientist and Engineer's Guide to Digital Signal Processing*, 351-372. San Diego, CA: California Technical Publishing, 1997.

Sicari, S., A. Rizzardi, L.A. Grieco, and A. Coen-Porisini. “Security, Privacy and Trust in Internet of Things: The Road Ahead.” *Computer Networks* 76 (2015): 146–164.

Srivastava, Lara et al. *The Internet of Things*. Geneva: International Telecommunications Union, 2005.

Stivers, Richard. “The Media Creates Us in Its Image.” *Bulletin of Science, Technology & Society* 32, 3 (2012): 203-212.

Stoycheff, Elizabeth. “Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring.” *Journalism & Mass Communication Quarterly* 14, 3 (2016)*:* 1–16.

Weiser, Mark. “The Computer for the 21st Century.” *Scientific American* 265, 3 (1991): 94–104.

Zuboff, Shoshana. “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization.” *Journal of Information Technology* 30, 1 (2015): 75–89.