Hello
Firstly, thank you to Electrofringe for inviting me to this years event "Your Privacy Is Important To Us".

I'm going to talk about a research project called PilferShush, that examines one of the hidden methods that the Internet-of-Things uses to communicate with mobile phones and how its unregulated spread can challenge the way we think about public and private space.

This hidden method is the broadcast of inaudible sounds from IoT devices and services. The purpose of using such hidden sounds is to identify the person and their phone without our awareness.

Understanding this process may reveal the current scale of internet based surveillance.

==========

PROJECT SPECIFIC

The Internet-of-Things has been around for over a decade and consists of small devices, digital sensors, a processing unit and an internet connection.

From rainfall measuring devices in national parks to a set of shoes in a High Street shop, they are designed to "anticipate human needs based on information collected about their context" (ITU, 2005).

The arrival of the IoT environment means that we cannot simply avoid these technologies, they surround us.

For several years, IoT devices have been able to connect to our mobile phones via near ultra high frequency audio signals. These signals can be transmitted by any standard speaker system and can be heard and decoded by any phone.

These inaudible sounds consist of multiple tones starting from 18 kilohertz, with each tone lasting several milliseconds, like a sped up version of morse code. The series of tones can be understood as saying this is my unique ID, if you have my software then connect to my server and let it log your identity.

When this technique is performed on your phone, there is no visible sign of its occurrence. So you have no knowledge or power over this exchange nor the chance to comprehend what information is being sent and to whom.

Further obscuring this process, IoT devices are hidden in everyday objects.

So that pair of shoes in a shop aren't simply for wearing on your feet. Instead, they are an IoT device that will inform a multinational corporation that you are nearby. Find out who you are, where you have been and what you like. And then via a pop up advert or sponsored post, suggest a suitable wine from a nearby bottleshop to go with that dinner it "thinks" you typically eat on a Thursday evening.

==========

PRIVACY

Today's urban landscape is filled with creepy teddy bears, billboards that identify you, televisions that watch you and phones that will always listen to what you say. Combined they form part of a massive evolution in the way technology defines the economy and mediates social relations.

Determining WHO is doing WHAT, WHERE and WHEN is one of the most pervasive behaviours in contemporary society: from antagonistic governments, to profit-seeking corporations and finally to our voyeuristic selves.

The techno-absolutism performed by the CEOs of Silicon Valley and start-up entrepreneurs is matched by our own techno-fetishism. We adopt new technology, voraciously, uncritically and sycophantically.

We have a fascination with quantifying the self, and of reducing as many things as possible into digital descriptions. We are doing this and allowing unaccountable software to determine the access we have to our own digital society.

Corporate control over the mediums of communication operate via mechanisms such as intellectual property, company law, proprietary software and patented technologies. When corporations deploy new technologies they demonstrate that

"rapid abilities to surveil for profit outrun public understanding". The communication surveillance taking place now is merely a precursor to a future in which a corporation will think it "know[s] what you want and tell you before you ask the question".

Prior to Cambridge Analytica's contextual manipulation of personal data, an example of this control can be found in Facebook's Massive Scale Emotional Contagion experiment. This example also demonstrates the power imbalance at the heart of most relationships between us and corporations.

In 2014 the platform edited emotional expressions in the posts of over one hundred and fifty five thousand people. This editing was performed with the intention of manipulating and transferring either a positive or negative emotional state to its users. Despite none of these users being aware of this occurring, Facebook said that informed consent was given as part of the user agreement made when people sign up for a Facebook account.

In response to concerns people may have 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".

To provide that something, the corporation "has to know a lot about you and your environment to provide these services". The provision of this information is achieved by data generated on the internet, a technology "that is also regarded by most people as essential for basic social participation". Somewhere in this lies the concept of privacy, a right to privacy and the normative behaviour that seems to offer tacit approval for privacy violations. (Shoshana Zuboff)

==========

And after all that, we are left to ask what does PRIVACY mean? 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.

This in turn also highlights one of the difficulties in articulating privacy rights, it is often only apparent after a violation has occurred.

A coherent definition of privacy might be more easily reached in the "context not only of place, but of politics, convention, and cultural expectation". It is within contexts such as these and the merging of their boundaries in the age of "smart phones", the "sharing economy" and ubiquitous internet connections, that we now find ourselves. (Helen Nissenbaum)

In the early idealistic days of the web it was thought that an online identity was something "that was easily put on and taken off while the Internet guaranteed anonymity". Today we can imagine these two identities to be interchangeable and that the anonymity once provided can no longer be guaranteed.

The merging of digital and analogue identities combine in such a way that they "co-create the experience of identity". The influence of one over the other is apparent when we consider that these two sides of identity are so closely entwined. (J. Sage Elwell)

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". The theory known as "surveillance capitalism" demonstrates that it is now possible to "predict and modify" as well as "observe behaviour that was previously unobservable and write contracts on it".

This is performed at the corporate level through "incursions into undefended private territory until resistance is encountered". 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". Its application reveals that information is extracted "without knowledge, consent, or rights of privacy". It also reveals one of the most pernicious aspects of a technological infringement of privacy in that when it takes place we are typically not even aware of its occurrence. (Shoshana Zuboff)

==========

TRACKERS

The deriving of profit from digitised identities, behaviours and actions has seen the rise of outsourcing of labour at the forefront of the digital economy. From the isolated and speculative income of the Uber driver and the unprotected food delivery rider, to the access of vital social services via online apps; the sharing economy socialises the risks, debts and running costs while privatising the profits.

One method to extract profit from human digital labour is to digitise the Time and Motion surveillance of the factory into software known as trackers. This type of software is typically made available for developers to include within their apps. It can provide a source of revenue via the exchange of gleaned statistics about who is using the app and how.

Companies profit from this type of information by connecting the capabilities of tracker software with massive relational databases. These databases exist for the specific purpose of identifying people, their behaviours and their traits. And from here the professed intention is to anticipate "your needs" before you are aware of them.

==========

WHY IS IT A CONCERN

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". And, perhaps more importantly, that surveillance can "influence conformist behaviour". (Elizabeth Stoycheff)

This is based upon an agreed understanding that "public opinion is the opinion which can be voiced in public without fear of sanctions".
(Elisabeth Noelle-Neumann)

These concepts may seem far removed from an environment containing IoT sensors. But surveillance technology and the IoT that performs that role, generates data that is used by both government and corporate actors to identify people and their characteristics. And this information in turn allows those with power and access to influence and control.

Ultimately, the specifics of a particular technology is not what is relevant; It is the context within which it operates that matters.

A single seemingly insignificant piece of information is taken out of its context and combined with a multitude of others. Together they provide a picture of the person. Whether this digitised picture is accurate, warranted or even malleable is something we are not able to ascertain. Nor are we able to exercise control over its acquisition and nor are we able to limit or control its use.

This is operating within the context of an economic ideology that seeks to turn all it touches into virtual gold. It does so using the same language now as it did hundreds of years ago: by "mining" a resource, "extracting" raw material and "converting" everything it can into a commodity that can be auctioned. In the digital economy that resource is you and the raw material is your role within that economy. And controlling you is vital to governments, as much as influencing you is desired by corporations.

==========

REFS::

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.

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.

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

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.

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